NETGEAR ProSafe Dual Band Wireless Access Point WAG302 Reference Manual (802.11a/g)

NETGEAR®

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10181-02
May 2006

Technical Support

Please register to obtain technical support. Please retain your proof of purchase and warranty information.

To register your product, get product support or obtain product information and product documentation, go to *http://www.NETGEAR.com*. If you do not have access to the World Wide Web, you may register your product by filling out the registration card and mailing it to NETGEAR customer service.

You will find technical support information at: *http://www.NETGEAR.com/* through the customer service area. If you want to contact technical support by telephone, see the support information card for the correct telephone number for your country.

© 2006 by NETGEAR, Inc. All rights reserved.

Trademarks

NETGEAR and the NETGEAR logo are registered trademarks, and ProSafe is a trademark, of NETGEAR, INC. Windows is a registered trademark of Microsoft Corporation. Other brand and product names are trademarks or registered trademarks of their respective holders. Information is subject to change without notice. All rights reserved.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Modifications made to the product, unless expressly approved by Netgear, could void the user's authority to operate the equipment. NETGEAR does not assume any liability that may occur due to such condition.

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

ProSafe 802.11a/g Dual Band Wireless Access Point

Tested to Comply
with FCC Standards
FOR HOME OR OFFICE USE

FCC ID: PY3WAG302

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

Placement and Range Guidelines

Indoors, computers can connect over 802.11 wireless networks at a maximum range of 500 feet (152.4 m) for 802.11b devices. However, the operating distance or range of your wireless connection can vary significantly, based on the physical placement of the wireless access point.

For best results, identify a location for your wireless access point according to these guidelines:

- Away from potential sources of interference, such as PCs, large metal surfaces, microwaves, and 2.4 GHz cordless phones.
- In an elevated location such as a high shelf that is near the center of the wireless coverage area for all mobile devices.

Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the wireless access point.

To meet FCC and other national safety guidelines for RF exposure, the antennas for this device must be installed to ensure a minimum separation distance of 20cm (7.9 in.) from persons. Further, the antennas shall not be collocated with other transmitting structures.

FCC Statement

DECLARATION OF CONFORMITY

We Netgear,
4500 Great America Parkway
Santa Clara, CA 95054, USA
Tel: +1 408 907 8000
declare under our sole responsibility that the product(s)
WAG302 *(Model Designation)*
802.11a/g ProSafe™ Dual Band Wireless Access Point *(Product Name)*
complies with Part 15 of FCC Rules.

Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices)

FCC Requirements for Operation in the United States

Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

- Reorient or locate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

RF Exposure Warning for North America, and Australia

Warning! To meet FCC and other national safety guidelines for RF exposure, the antennas for this device (see below) must be installed to ensure a minimum separation distance of 20cm (7.9 in.) from persons. Further, the antennas shall not be collocated with other antenna or radio transmitter.

Antenna Statement for North America and Australia

In addition to its own 2 antennas, the WAG302 device has been approved for use with the following detachable antennas and antenna cables:

Approved Antennas	Antenna Gain and type	Approved Antenna Cable	Antenna Cable Length	Maximum Transmitted Power
NETGEAR ANT24D18	18 dBi, directional outdoor/indoor	NETGEAR ACC-10314-01 thru 05	1.5 m to 30 m	19 dBm + 18 dBi ant.
NETGEAR ANT2409	9 dBi, omnidirectional outdoor/indoor	NETGEAR ACC-10314-01 thru 05	1.5 m to 30 m	19 dBm + 9 dBi ant.
NETGEAR ANT24O5	5 dBi, ceiling/wall indoor	NETGEAR ACC-10314-01 thru 05	1.5 m to 30 m	19 dBm + 5 dBi ant.

*****WG302 maximum radiated power in North America and Australia: 20 dBm – cable loss + antenna gain

Please go to *www.netgear.com/go/wag302_fcc* for an updated list of wireless accessories approved to be used with the WAG302 in North America and Australia.

Industry Canada Compliance Statement

This Class B Digital apparatus meets all the requirements of the Canadian Interference Causing Equipment Regulations ICES 003.

Cet appareil numerique de classe B respecte les exigences du reglement du Canada sur le materiel brouilleur NMB-003.

The device is certified to the requirements of RSS-210 for 2.4 GHz spread spectrum devices. The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations. For further information, contact your local Industry Canada office.

Europe – EU Declaration of Conformity

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN300 328, EN301 489-17, EN60950Europe – Declaration of Conformity in Languages of the European Community

Èesky [Czech]	*NETGEAR Inc.* tímto prohlašuje, _e tento Radiolan je ve shodě se základními po_adavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede *NETGEAR Inc.* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *NETGEAR Inc.*, dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab *NETGEAR Inc.* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *NETGEAR Inc.*, declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente *NETGEAR Inc.* declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Åëëçíéêþ [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *NETGEAR Inc.* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente *NETGEAR Inc.* déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente *NETGEAR Inc.* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *NETGEAR Inc.* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuviø [Lithuanian]	Šiuo *NETGEAR Inc.* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *NETGEAR Inc.* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, *NETGEAR Inc.*, jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.

Magyar [Hungarian]	Alulírott, *NETGEAR Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	*NETGEAR Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*NETGEAR Inc.* týmto vyhlasuje, _e Radiolan spĺňa základné po_iadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	*NETGEAR Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar *NETGEAR Inc.* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [Icelandic]	Hér með lýsir *NETGEAR Inc.* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	*NETGEAR Inc.* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

Countries of Operation & Conditions of Use in the European Community

This device is intended to be operated in all countries of the European Community. Requirements for indoor vs. outdoor operation, license requirements and allowed channels of operation apply in some countries as described below.

Note: The user must use the configuration utility provided with this product to ensure the channels of operation are in conformance with the spectrum usage rules for European Community countries as described below.

This device requires that the user or installer properly **enter the current country of operation** in the 5GHz Radio Configuration Window as described in the user guide, **before operating this device**.

This device will automatically limit the allowable channels determined by the current country of operation. Incorrectly entering the country of operation may result in illegal operation and may cause harmful interference to other system. The user is obligated to ensure the device is operating according to the channel limitations, indoor/outdoor restrictions and license requirements for each European Community country as described in this document.

This device employs **a radar detection feature** required for European Community operation in the 5GHz band. This feature is automatically enabled when the country of operation is correctly configured for any European Community country. The presence of nearby radar operation may result in temporary interruption of operation of this device. The radar detection feature will automatically restart operation on a channel free of radar.

The **5GHz Turbo Mode** feature is not allowed for operation in any European Community country. The current setting for this feature is found in the 5GHz Radio Configuration Window as described in the user guide.

This device may be operated **indoors or outdoors** in all countries of the European Community using the 2.4GHz band: Channels 1 – 13, except where noted below:

- In **Italy** the end-user must apply for a license from the national spectrum authority to operate this device outdoors.

- In **France** outdoor operation is only permitted using the 2.4 – 2.454 GHz band: Channels 1 – 7.
- **Belgium** requires notifying spectrum agency if deploying >300meter wireless links in outdoor public areas using 2.4GHz band.

European Spectrum Usage Rules - Effective April 11, 2006				
Country	**5.15-5.25 (GHz) Channels: 36,40,44,48**	**5.25-5.35 (GHz) Channels: 52,56,60,64**	**5.47-5.725 (GHz) Channels: 100,104,108,112,116, 120,124,128,132,136,140**	**2.4-2.4835 (GHz) Channels: 1 to 13 (Except Where Noted)**
ALL EC Countries	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Belgium	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor !
France	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor Ch. 1-13 Outdoor 1-7 Only
Greece	Indoor Only	Indoor Only	Indoor Only	Indoor Only
Italy	Indoor Only	Indoor Only	Indoor (Outdoor w/License)	Indoor (Outdoor w/ License)
Turbo Mode	Not Allowed in 5GHz			Same 2.4 GHz rules as above
AdHoc Mode	Not Allowed			Same 2.4 GHz rules as above

Antenna Statement for the European Community

Please note that the 100mW EIRP limit and regulations could vary in Europe from country to country. Please check the regulations in your country. The antenna cable type and length must comply with European regulations. Refer to the table below for approved antenna and cable accessories.

In addition to its own antenna, the WAG302 device has been approved for use with the following detachable antennas and antenna cables:

Approved Antennas	**Antenna Gain and type**	**Approved Antenna Cable**	**Minimum Antenna Cable Length**	**Minimum Antenna Cable Attenuation**	**Maximum Transmitted Power[a]**
NETGEAR ANT24D18v2	14.5 dBi, directional outdoor/indoor	NETGEAR ACC-10314-05	30 m	18 dB	-3 dBm + 14.5 dBi = 15 dBm EIRP
NETGEAR ANT2409	9 dBi, omnidirectional outdoor/indoor	NETGEAR ACC-10314-04 or ACC-10314-05	10 m	6.1 dB	8.9 dBm + 9 dBi = 17.9 dBm EIRP
NETGEAR ANT24O5	5 dBi, ceiling/wall indoor	NETGEAR ACC-10314-01 thru 05	1.5 m	1.1 dB	14 dBm + 5 dBi = 19 dBm EIRP

a. WAG302 maximum radiated power in the European Community: 15 dBm – cable loss + antenna gain

Please go to *http://www.NETGEAR.com* and use the search feature to find an updated list of wireless accessories approved to be used with the WAG302 in the European Community.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das ProSafe 802.11a/g Dual Band Wireless Access Point WAG302 gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Certificate of the Manufacturer/Importer

It is hereby certified that the ProSafe 802.11a/g Dual Band Wireless Access Point WAG302 has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Product and Publication Details

Model Number:	WAG302
Publication Date:	May 2006
Product Family:	Wireless Access Point
Product Name:	ProSafe 802.11a/g Dual Band Wireless Access Point WAG302
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10181-02

Contents

About This Manual

Conventions, Formats and Scope xiii
How to Use This Manual xiv
How to Print this Manual xv

Chapter 1
Introduction

About the ProSafe 802.11a/g Dual Band Wireless Access Point WAG302 1-1
Key Features and Standards 1-2
Supported Standards and Conventions 1-2
Key Features 1-2
802.11a/g Standards-based Wireless Networking 1-4
Autosensing Ethernet Connections with Auto Uplink 1-4
Compatible and Related NETGEAR Products 1-5
System Requirements 1-5
What's In the Box? 1-5
Hardware Description 1-6
Front Panel 1-6
Rear Panel 1-8

Chapter 2
Basic Installation and Configuration

Wireless Equipment Placement and Range Guidelines 2-1
Understanding WAG302 Wireless Security Options 2-2
Installing the WAG302 Wireless Access Point 2-3
Setting up the WAG302 Wireless Access Point 2-4
Configuring LAN and Wireless Access 2-4
Deploying the WAG302 Wireless Access Point 2-9
Verifying Wireless Connectivity 2-9
Logging In Using the Default IP Address 2-10
Setting Basic IP Options 2-11

Wireless Settings 2-14
Configuring 802.11a Wireless Settings 2-14
Configuring 802.11b/g Wireless Settings 2-15
Setting Up and Testing Basic Wireless Connectivity 2-17
Understanding Security Profiles 2-18
SSID and WEP/WPA Settings Setup Form 2-22
802.11a Configuration 2-22
802.11b/g Configuration 2-23
Configuring the RADIUS Server Settings 2-24
Setting up a Security Profile 2-26
Configuring WEP 2-28
Configuring WPA with RADIUS 2-30
Configuring WPA2 with RADIUS 2-31
Configuring WPA and WPA2 with RADIUS 2-32
Configuring WPA-PSK 2-33
Configuring WPA2-PSK 2-34
Configuring WPA-PSK and WPA2-PSK 2-35
Restricting Wireless Access by MAC Address 2-36

Chapter 3
Management

Remote Management 3-1
Using the Secure Telnet Interface 3-2
CLI Commands 3-3
Using Syslog and Activity Log Information 3-3
Viewing General Summary Information 3-5
Viewing Network Traffic Statistics 3-8
Viewing Available Wireless Station Statistics 3-9
Upgrading the Wireless Access Point Software 3-10
Configuration File Management 3-11
Saving and Retrieving the Configuration 3-12
Restoring the WAG302 to the Factory Default Settings 3-13
Changing the Administrator Password 3-13

Chapter 4
Advanced Configuration

IP Settings for Wireless Clients 4-1

Hotspot Settings 4-3
Configuring Advanced Wireless Settings 4-3
Enabling Wireless Bridging and Repeating 4-5
Configuring a WAG302 as a Point-to-Point Bridge 4-7
Configuring a Point-to-Multi-Point Wireless Bridge 4-8
Configuring the WAG302 as a Wireless Repeater 4-9

Chapter 5
Troubleshooting

No lights are lit on the wireless access point. 5-1
The Wireless LAN activity light does not light up. 5-2
The LAN light is not lit. 5-2
I cannot access the Internet or the LAN with a wireless capable computer. 5-2
I cannot connect to the WAG302 to configure it. 5-3
When I enter a URL or IP address I get a timeout error. 5-3
Using the Reset Button to Restore Factory Default Settings 5-4

Appendix A
Default Settings and Technical Specifications

Factory Default Settings A-1
Technical Specifications A-3

Appendix B
Related Documents

Appendix C
Command Line Reference

Command Sets C-1

Index

About This Manual

The *NETGEAR® ProSafe™ Dual Band Wireless Access Point WAG302 Reference Manual (802.11a/g)* describes how to install, configure and troubleshoot the ProSafe 802.11a/g Dual Band Wireless Access Point WAG302.The information in this manual is intended for readers with intermediate computer and Internet skills.

Conventions, Formats and Scope

The conventions, formats, and scope of this manual are described in the following paragraphs:

- **Typographical Conventions.** This manual uses the following typographical conventions:

Italics	Emphasis, books, CDs, URL names
Bold	User input
`Fixed`	Screen text, file and server names, extensions, commands, IP addresses

- **Formats.**This manual uses the following formats to highlight special messages:

	Note: This format is used to highlight information of importance or special interest.

	Tip: This format is used to highlight a procedure that will save time or resources.

	Warning: Ignoring this type of note may result in a malfunction or damage to the equipment.

	Danger: This is a safety warning. Failure to take heed of this notice may result in personal injury or death.

- **Scope.** This manual is written for the WAG302 Wireless Access Point according to these specifications:

Product Version	ProSafe 802.11a/g Dual Band Wireless Access Point WAG302
Manual Publication Date	May 2006

For more information about network, Internet, firewall, and VPN technologies, see the links to the NETGEAR website in Appendix B, “Related Documents”.

	Note: Product updates are available on the NETGEAR, Inc. website at *http://kbserver.netgear.com/products/WAG302.asp*.

How to Use This Manual

The HTML version of this manual includes the following:

- Buttons, and , for browsing forwards or backwards through the manual one page at a time
- A button that displays the table of contents and an button. Double-click on a link in the table of contents or index to navigate directly to where the topic is described in the manual.
- A button to access the full NETGEAR, Inc. online knowledge base for the product model.
- Links to PDF versions of the full manual and individual chapters.

How to Print this Manual

To print this manual you can choose one of the following several options, according to your needs. Your computer must have the free Adobe Acrobat Reader installed in order to view and print PDF files. The Acrobat Reader is available on the Adobe website at *http://www.adobe.com*.

- **Printing a Page in the HTML View**. Each page in the HTML version of the manual is dedicated to a major topic. Use the *Print* button on the browser toolbar to print the page contents.
- **Printing a Chapter**. Use the *PDF of This Chapter* link at the top left of any page.
  - Click the *PDF of This Chapter* link at the top right of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.
  - Click the print icon in the upper left of the window.

Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

- **Printing the Full Manual**. Use the *Complete PDF Manual* link at the top left of any page.
  - Click the Complete PDF Manual link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.
  - Click the print icon in the upper left of the window.

Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Chapter 1
Introduction

This chapter describes some of the key features of the NETGEAR ProSafe 802.11a/g Dual Band Wireless Access Point WAG302. It also includes the minimum prerequisites for installation ("System Requirements" on page 1-5.), package contents ("What's In the Box?" on page 1-5) and a description of the front and back panels of the WAG302 ("Hardware Description" on page 1-6).

About the ProSafe 802.11a/g Dual Band Wireless Access Point WAG302

The ProSafe 802.11a/g Dual Band Wireless Access Point WAG302 is the basic building block of a wireless LAN infrastructure. It provides connectivity between Ethernet wired networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices.

The WAG302 provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage—interacting with a wireless network interface card (NIC) via an antenna. Typically, an individual in-building access point provides a maximum connectivity area of about a 300 foot radius. Consequently, the ProSafe 802.11a/g Dual Band Wireless Access Point WAG302 can support a small group of users in a range of several hundred feet. Most access points can handle between 10 to 30 users simultaneously.

The ProSafe 802.11a/g Dual Band Wireless Access Point WAG302 acts as a bridge between the wired LAN and wireless clients. Connecting multiple WAG302 Wireless Access Points via a wired Ethernet backbone can further lengthen the wireless network coverage. As a mobile computing device moves out of the range of one access point, it moves into the range of another. As a result, wireless clients can freely roam from one Access Point to another and still maintain seamless connection to the network.

The auto-sensing capability of the ProSafe 802.11a/g Dual Band Wireless Access Point WAG302 allows packet transmission at up to 108 Mbps, or at reduced speeds to compensate for distance or electromagnetic interference.

Key Features and Standards

The WAG302 Wireless Access Point is easy-to-use and provides solid wireless and networking support. It also offers a wide range of security options.

Supported Standards and Conventions

The following standards and conventions are supported:

- **Standards Compliant.** The Wireless Access Point complies with the IEEE 802.11a/g for Wireless LANs.
- **WEP support.** Support for WEP is included. 64-bit, 128-bit, and 152-bit keys are supported.
- **Full WPA and WPA2 support.** WPA and WPA2 enterprise-class strong security with RADIUS and certificate authentication as well as dynamic encryption key generation.WPA-PSK and WPA2-PSK preshared key authentication without the overhead of RADIUS servers but with all of the strong security of WPA.
- **Multiple BSSIDs.** Supports multiple BSSIDs. When one wireless access point is connected to a wired network and a set of wireless stations, it is called a Basic Service Set (BSS). The Basic Service Set Identifier (BSSID) is a unique identifier attached to the header of packets sent over a WLAN that differentiates one WLAN from another when a mobile device tries to connect to the network.
- **DHCP Client Support.** DHCP provides a dynamic IP address to PCs and other devices upon request. The WAG302 can act as a client and obtain information from your DHPC server; it can also act as a DHCP server and provide network information for wireless clients.
- **SNMP Support.** Support for Simple Network Management Protocol (SNMP) Management Information Base (MIB) management.
- **802.1Q VLAN (Viral Wireless LAN) Support.** A network of computers that behave as if they are connected to the same network even though they actually may be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible. VLANs are very useful for user/host management, bandwidth allocation and resource optimization.

Key Features

The WAG302 provides solid functionality, including these features:

- Multiple Operating Modes

  - **Wireless Access Point.** Operates as a standard 802.11a/g.
  - **Point-to-Point Bridge.** In this mode, the WAG302 only communicates with another bridge-mode wireless station. Network authentication should be used to protect this communication.
  - **Point-to-Multi-Point Bridge.** Select this only if this WAG302 is the "Master" for a group of bridge-mode wireless stations. The other bridge-mode wireless stations send all traffic to this "Master", and do not communicate directly with each other. Network Authentication should be used to protect this traffic.
  - **Wireless Repeater.** In this half-duplex mode, the WAG302 only communicates with another repeater-mode wireless station. Network authentication should be used to protect this communication.

- **Hotspot Settings.** You can allow all HTTP (TCP, port 80) requests to be captured and redirected to the URL you specify.
- **Upgradeable Firmware.** Firmware is stored in a flash memory and can be upgraded easily, using only your Web browser, and can be upgraded remotely.
- **Access Control.** The Access Control MAC address filtering feature can ensure that only trusted wireless stations can use the WAG302 to gain access to your LAN.
- **Security Profiles.** When using multiple BSSIDs, you can configure unique security settings (encryption, SSID, etc.) for each BSSID.
- **Simple Configuration.** If the default settings are unsuitable, they are easy to change.
- **Hidden Mode.** The SSID is not broadcast, assuring only clients configured with the correct SSID can connect.
- **Secure Telnet Command Line Interface.** The Telnet command line interface enables direct access over the serial port and easy scripting of configuration of multiple WAG302 across an extensive network via the Ethernet interface. An SSH client is required.
- **Configuration Backup.** Configuration settings can be backed up to a file and restored.
- **Secure and Economical Operation.** Adjustable power output allows more secure or economical operation.
- **Power over Ethernet.** Power can be supplied to the WAG302 over the Ethernet port from any 802.3af compliant mid-span or end-span source such as the NETGEAR FSM7326P Managed Power over Ethernet Layer 3 managed switch.
- **Autosensing Ethernet Connection with Auto Uplink lnterface.** Connects to 10/100 Mbps IEEE 802.3 Ethernet networks.

- **LED Indicators.** Power, test, LAN speed, LAN activity, and wireless activity are easily identified.
- **Wireless Multimedia (WMM) Support.** WMM is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the kind of data. Time-dependent information, like video or audio, has a higher priority than normal traffic. For WMM to function correctly, Wireless clients must also support WMM.
- **Quality of Service (QoS) Support.** You can configure parameters that affect traffic flowing from the wireless access point to the client station and traffic flowing from the client station to the wireless access point. The QoS feature allows you to prioritize traffic, such as voice and video traffic, so that packets do not get dropped.Compatible and Related NETG.
- **VLAN Security Profiles.** Each Security Profile is automatically allocated a VLAN ID as each Security Profile is modified.

802.11a/g Standards-based Wireless Networking

The ProSafe 802.11a/g Dual Band Wireless Access Point WAG302 provides a bridge between Ethernet wired LANs and 802.11a/g compatible wireless LAN networks. It provides connectivity between Ethernet wired networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices. Additionally, the WAG302 supports the following wireless features:

- Distributed coordinated function (CSMA/CA, Back off procedure, ACK procedure, retransmission of unacknowledged frames)
- RTS/CTS handshake
- Beacon generation
- Packet fragmentation and reassembly
- Short or long preamble
- Roaming among access points on the same subnet

Autosensing Ethernet Connections with Auto Uplink

The WAG302 can connect to a standard Ethernet network. The LAN interface is autosensing and capable of full-duplex or half-duplex operation.

The wireless access point incorporates Auto Uplink™ technology. The Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a “normal” connection such as to a computer or an “uplink” connection such as to a switch or hub. That port

will then configure itself to the correct configuration. This feature also eliminates any concerns about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection.

Compatible and Related NETGEAR Products

For a list of compatible products from other manufacturers, see the Wireless Ethernet Compatibility Alliance Web site (WECA, see *http://www.wi-fi.net*).

The following NETGEAR products work with the WAG302 Wireless Access Point:

- WAG511 ProSafe 108 Mbps Dual Band PC Card
- WAG311 ProSafe 108 Mbps Dual Band PCI Card
- WG311T 802.11g 108 Mbps Wireless PCI Card
- WG511T 802.11g 108 Mbps Wireless CardBus Adapter
- WG511 802.11g 54 Mbps Wireless CardBus Adapter
- WG111 801.11g 54 Mbps Wireless USB Adapter

System Requirements

Before installing the WAG302, make sure your system meets these requirements:

- A 10/100 Mbps Local Area Network device such as a hub or switch
- The Category 5 UTP straight through Ethernet cable with RJ-45 connector included in the package, or one like it
- A 100-240 V, 50-60 HZ AC power source
- A Web browser for configuration such as Microsoft Internet Explorer 6.0 or above, or Netscape Navigator 4.78 or above
- At least one computer with the TCP/IP protocol installed
- 802.11b or 802.11b-compliant devices, such as the NETGEAR WG511 Wireless Adapter

What's In the Box?

The product package should contain the following items:

- ProSafe 802.11a/g Dual Band Wireless Access Point WAG302

- Power adapter and cord (12 V dc, 1.2 A)
- Straight through Category 5 Ethernet cable
- NETGEAR WAG302 802.11a/g Dual Band Wireless Access Point Installation Guide
- *Resource CD* which includes this manual.
- Support Registration card

Contact your reseller or customer support in your area if there are any missing or damaged parts. You can refer to the Support Information Card for the telephone number of customer support in your area. You should keep the Support Information card, along with the original packing materials, and use the packing materials to repack the WAG302 if you need to return it for repair. To qualify for product updates and product warranty registrations, we encourage you to register on the NETGEAR Web site at: *http://www.NETGEAR.com*.

Hardware Description

This section describes the front and rear hardware functions of the WAG302.

Front Panel

The WAG302 front hardware functions are described below.

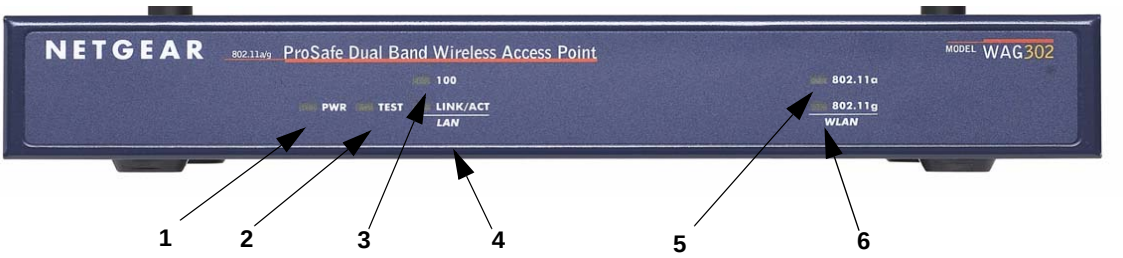


Figure 1-1

The following table explains the LED indicators:

Table 1-1. Front Panel LED Indicators

Item	LED		DESCRIPTION
1	**PWR**		Power Indicator
		Off	No power.
		On	Power is on.
2	**TEST**		Self Test Indicator
		Blink	Indicates self test, loading software, or system fault (if continues). Note: This LED may blink for a minute before going off.
3	**100**		Ethernet LAN Speed Indicator
		Off	Indicates 10 Mbps Ethernet link detected
		On (Green)	100 Mbps Fast Ethernet link detected.
4	**LINK/ACT LAN**		Ethernet LAN Link Activity Indicator
		Off	Indicates no Ethernet link detected.
		On (Green)	100 Mbps Fast Ethernet link detected, no activity.
		Blink (Green)	Indicates data traffic on the 100Mbps Ethernet LAN.
		On (Amber)	10 Mbps Ethernet link detected, no activity.
		Blink (Amber)	Indicates data traffic on the 10Mbps Ethernet LAN.
5	**802.11a WLAN**		Wireless LAN Link Activity Indicator (5 GHz)
		Off	Indicates no wireless link activity.
		Blink (Green)	Wireless link activity.
6	**802.11g WLAN**		Wireless LAN Link Activity Indicator (2.4 GHz)
		Off	Indicates no wireless link activity.
		Blink (Green)	Wireless link activity.

Rear Panel

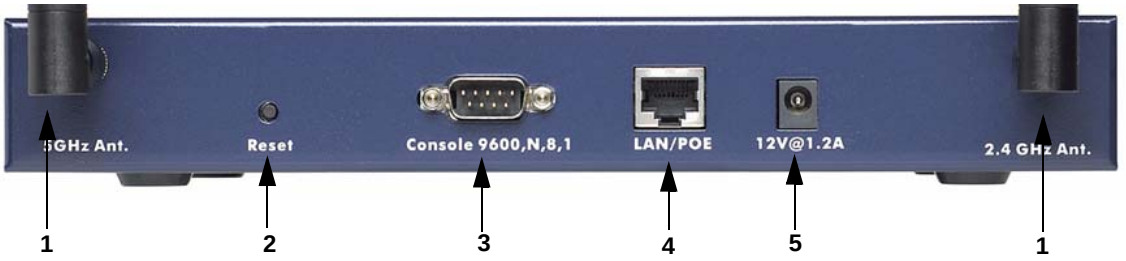


Figure 1-2

The WAG302 rear panel functions are described below:

1. Left and Right Detachable Antenna

   The WAG302 provides two detachable antennas (5 GHz and 2.4 GHz).

2. Restore to Factory Defaults Button

   The restore to default button located between the Ethernet RJ-45 connector and the power socket restores the WAG302 to the factory default settings.

3. Serial Console Port

   Male DB-9 serial port for serial DTE connections.

4. RJ-45 Ethernet Port

   Use the WAG302 Ethernet RJ-45 port to connect to an Ethernet LAN through a device such as a hub, switch, router, or POE switch.

5. Power Socket

   This socket connects to the WAG302 12V 1.2A power adapter.

Chapter 2
Basic Installation and Configuration

This chapter describes how to set up your ProSafe 802.11a/g Dual Band Wireless Access Point WAG302 for wireless connectivity to your LAN. This basic configuration will enable computers with 802.11b or 802.11a/g wireless adapters to do such things as connect to the Internet, or access printers and files on your LAN.

Note: Indoors, computers can connect over 802.11b or 802.11a/g wireless networks at ranges of several hundred feet or more. This distance can allow for others outside your area to access your network. It is important to take appropriate steps to secure your network from unauthorized access. The WAG302 Wireless Access Point provides highly effective security features which are covered in detail in "Understanding Security Profiles" on page 2-18. Deploy the security features appropriate to your needs

You need to prepare these three things before you can establish a connection through your wireless access point:

- A location for the WAG302 that conforms to the "Wireless Equipment Placement and Range Guidelines" below.
- The wireless access point connected to your LAN through a device such as a hub, switch, router, or Cable/DSL gateway.
- One or more computers with properly configured 802.11b or 802.11a/g wireless adapters.

Wireless Equipment Placement and Range Guidelines

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless access point. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices.

	Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the WAG302. For complete performance specifications, see Appendix A, "Default Settings and Technical Specifications."

For best results, place your wireless access point:

- Near the center of the area in which your PCs will operate.
- In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls).
- Away from sources of interference, such as PCs, microwaves, and 2.4 GHz cordless phones.
- Away from large metal surfaces.

Putting the antenna in a vertical position provides best side-to-side coverage. Putting the antenna in a horizontal position provides best up-and-down coverage.

If using multiple access points, it is better if adjacent access points use different radio frequency Channels to reduce interference. The recommended Channel spacing between adjacent access points is 5 Channels (for example, use Channels 1 and 6, or 6 and 11).

The time it takes to establish a wireless connection can vary depending on both your security settings and placement. Some types of security connections can take slightly longer to establish and can consume more battery power on a notebook computer.

Understanding WAG302 Wireless Security Options

Your wireless data transmissions can be received well beyond your walls by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The WAG302 Wireless Access Point provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

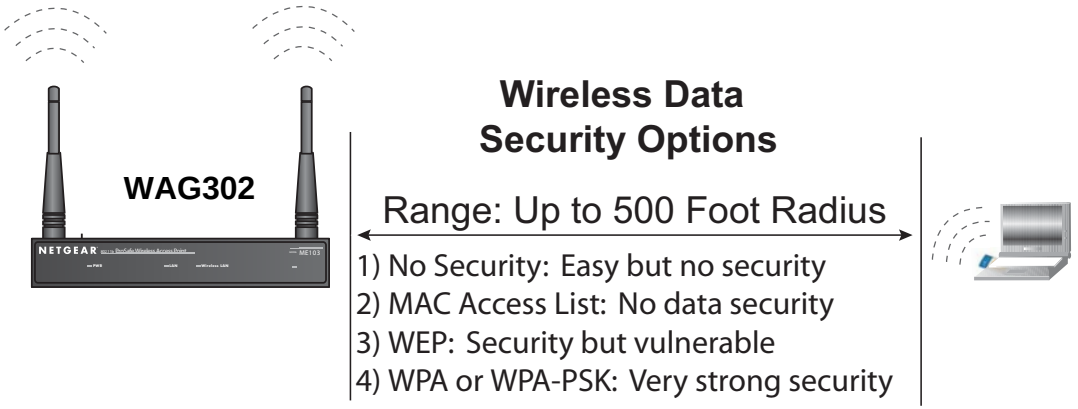


Figure 2-1

There are several ways you can enhance the security of your wireless network:

- **Restrict Access Based on MAC address.** You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the WAG302. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- **Turn Off the Broadcast of the Wireless Network Name (SSID).** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network "discovery" feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers.
- **Use WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption will block all but the most determined eavesdropper.
- **Use WPA or WPA-PSK.** Wi-Fi Protected Access (WPA) data encryption provides data security. The very strong authentication along with dynamic per frame rekeying of WPA make it virtually impossible to compromise. Because this is a new standard, wireless device driver and software availability may be limited.

Installing the WAG302 Wireless Access Point

Before installing the ProSafe 802.11a/g Dual Band Wireless Access Point WAG302, you should make sure that your Ethernet network is up and working. You will be connecting the access point to the Ethernet network so that computers with 802.11b or 802.11a/g wireless adapters will be able

to communicate with computers on the Ethernet network. In order for this to work correctly, verify that you have met all of the system requirements, shown on "System Requirements" on page 1-5.

Setting up the WAG302 Wireless Access Point

Tip: Before mounting the WAG302 in a high location, first set up and test the WAG302 to verify wireless network connectivity.

To set up the WAG302 Wireless Access Point:

1. Prepare a computer with an Ethernet adapter. If this computer is already part of your network, record its TCP/IP configuration settings.
2. Configure the computer with a static IP address of 192.168.0.210 and 255.255.255.0 for the Subnet Mask.
3. Connect an Ethernet cable from the WAG302 to the computer.
4. Turn on your computer, connect the power adapter to the WAG302 and verify the following:
   - The PWR power light goes on.
   - The LAN light of the wireless access point is lit when connected to a powered on computer.
   - The WLAN LEDs should be blinking.

Configuring LAN and Wireless Access

To configure the WAG302 Ethernet port for LAN access:

1. Connect to the WAG302 by opening your browser and entering **http://192.168.0.230** in the address field. The WAG302 login screen will appear.
2. Enter **admin** for the user name and **password** for the password, both in lower case letters as shown in Figure 2-2.

Figure 2-2

3. Click **Login now**. The main menu of the WAG302 will display as shown in Figure 2-3.

   - When the wireless access point is connected to the Internet, select the Documentation link under the Web Support menu to view the documentation for the wireless access point.
   - Select Logout to exit the WAG302 setup screens. (You will automatically be logged out of the wireless access point after 5 minutes of no activity.)

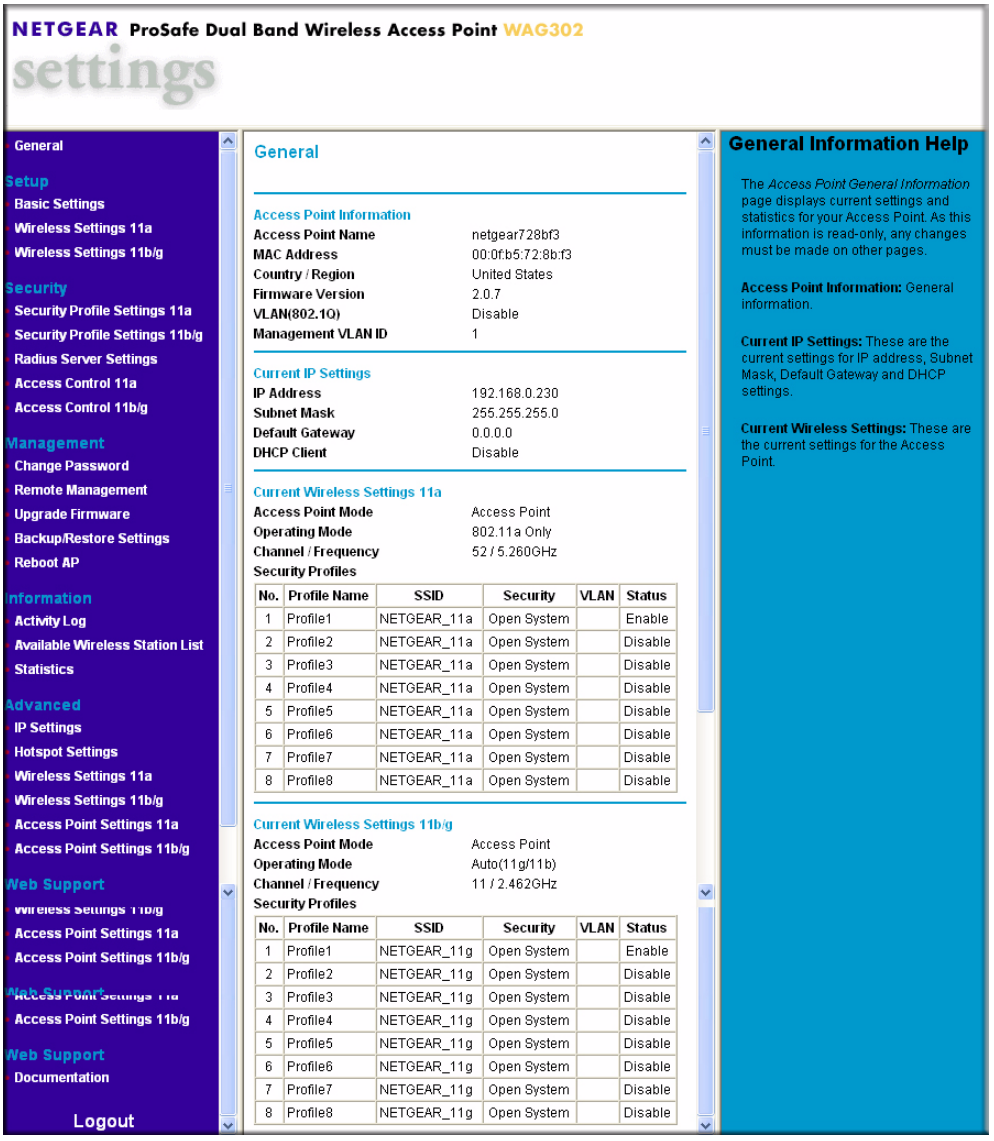
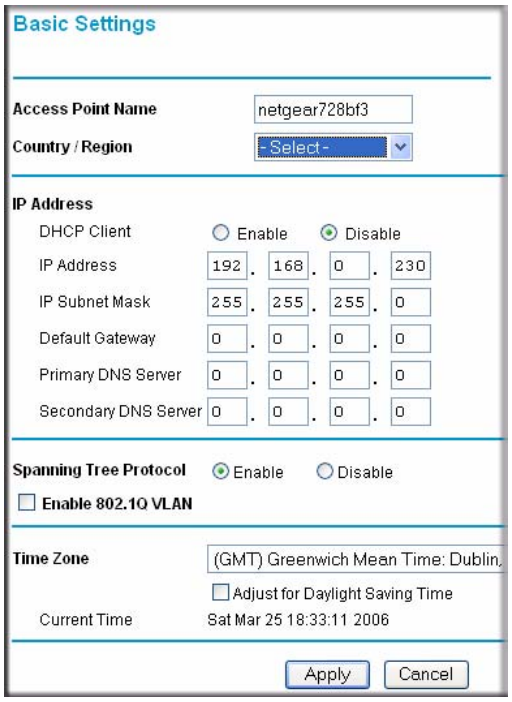

NETGEAR ProSafe Dual Band Wireless Access Point WAG302
settings
General
Setup
Basic Settings
Wireless Settings 11a
Wireless Settings 11b/g
Security
Security Profile Settings 11a
Security Profile Settings 11b/g
Radius Server Settings
Access Control 11a
Access Control 11b/g
Management
Change Password
Remote Management
Upgrade Firmware
Backup/Restore Settings
Reboot AP
Information
Activity Log
Available Wireless Station List
Statistics
Advanced
IP Settings
Hotspot Settings
Wireless Settings 11a
Wireless Settings 11b/g
Access Point Settings 11a
Access Point Settings 11b/g
Web Support
Access Point Settings 11a
Access Point Settings 11b/g
Web Support
Documentation
Logout
General
Access Point Information
Access Point Name netgear728bf3
MAC Address 00:0f:b5:72:8b:f3
Country / Region United States
Firmware Version 2.0.7
VLAN(802.1Q) Disable
Management VLAN ID 1
Current IP Settings
IP Address 192.168.0.230
Subnet Mask 255.255.255.0
Default Gateway 0.0.0.0
DHCP Client Disable
Current Wireless Settings 11a
Access Point Mode Access Point
Operating Mode 802.11a Only
Channel / Frequency 52 / 5.260GHz
Security Profiles
No. Profile Name SSID Security VLAN Status
1 Profile1 NETGEAR_11a Open System Enable
2 Profile2 NETGEAR_11a Open System Disable
3 Profile3 NETGEAR_11a Open System Disable
4 Profile4 NETGEAR_11a Open System Disable
5 Profile5 NETGEAR_11a Open System Disable
6 Profile6 NETGEAR_11a Open System Disable
7 Profile7 NETGEAR_11a Open System Disable
8 Profile8 NETGEAR_11a Open System Disable
Current Wireless Settings 11b/g
Access Point Mode Access Point
Operating Mode Auto(11g/11b)
Channel / Frequency 11 / 2.462GHz
Security Profiles
No. Profile Name SSID Security VLAN Status
1 Profile1 NETGEAR_11g Open System Enable
2 Profile2 NETGEAR_11g Open System Disable
3 Profile3 NETGEAR_11g Open System Disable
4 Profile4 NETGEAR_11g Open System Disable
5 Profile5 NETGEAR_11g Open System Disable
6 Profile6 NETGEAR_11g Open System Disable
7 Profile7 NETGEAR_11g Open System Disable
8 Profile8 NETGEAR_11g Open System Disable
General Information Help
The Access Point General Information page displays current settings and statistics for your Access Point. As this information is read-only, any changes must be made on other pages.
Access Point Information: General information.
Current IP Settings: These are the current settings for IP address, Subnet Mask, Default Gateway and DHCP settings.
Current Wireless Settings: These are the current settings for the Access Point.

Figure 2-3

4. Select Basic Settings on left side of the main menu. The Basic Settings screen will display.

Rest of World



United States

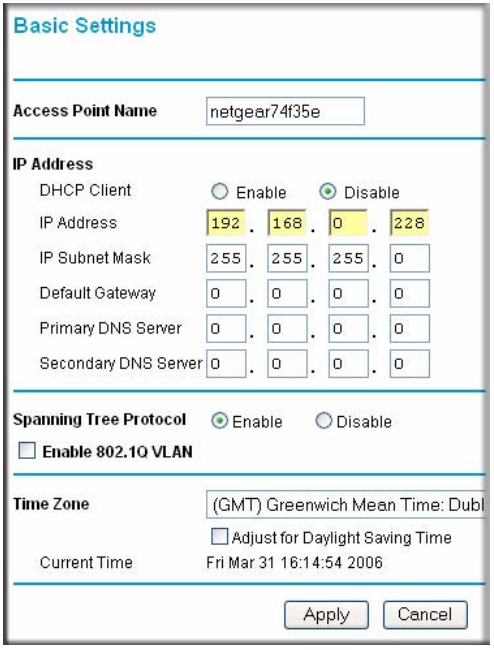


Figure 2-4

5. Select the Country/Region for your area (in the United States, the Country/Region is preset).)

> **Note:** You must set the Regulatory Domain. It may not be legal to operate the wireless access point in a region other than one of those identified in this field

6. Configure the IP Address settings appropriate for your network. The default values are suitable for most users and situations. (See the online help or "Setting Basic IP Options" on page 2-11 for more information about how to configure the settings on this screen.
7. Enable 802.1Q VLAN, if required. (This option is only useful if the hubs/switches on your LAN support the VLAN 802.1Q standard. If so, you can enable this feature.
8. Click **Apply.**

To configure your wireless settings for 11a and 11b/g:

1. From the main menu under Setup, select Wireless Settings11a. The Wireless Settings 11a screen will display.
2. Enter the wireless settings for your area. See the online help or "Configuring 802.11a Wireless Settings" on page 2-14.
3. Click **Apply.**

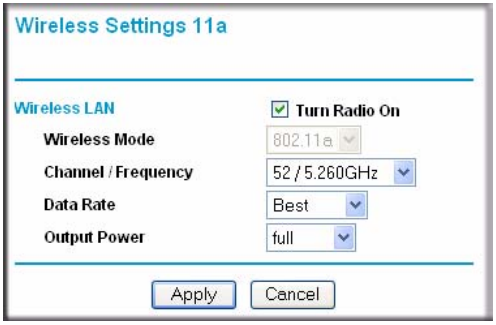


Figure 2-5

4. From the main menu under Setup, select Wireless Settings 11b/g. The Wireless Settings 11b/g screen will display.
5. Enter the wireless settings for your area. See the online help or "Configuring 802.11b/g Wireless Settings" on page 2-15.
6. Click **Apply** to save your settings.

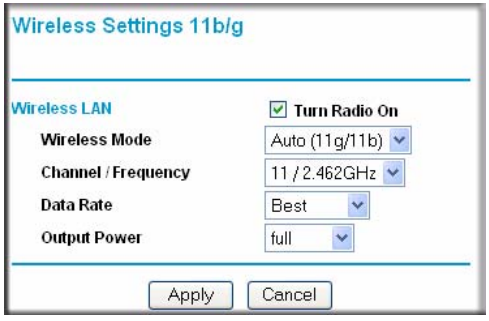


Figure 2-6

When you have completed the setup steps, you can deploy the WAG302 in your network. If needed, you can now reconfigure the computer you used in step 1 (from the Static IP) back to its original TCP/IP settings.

Deploying the WAG302 Wireless Access Point

To deploy the WAG302 Wireless Access Point:

1. Disconnect the WAG302 and position it where it will be deployed. The best location is elevated, such as wall mounted or on the top of a cubicle, at the center of your wireless coverage area, and within line of sight of all the mobile devices.
2. Lift the antenna on either side so that they are vertical.

> **Note:** Consult the antenna positioning and wireless mode configuration information in the Advanced Configuration chapter of the Reference Manual.

3. Connect an Ethernet cable from your WAG302 Wireless Access Point to a LAN port on your router, switch, or hub.

> **Note:** By default, WAG302 is set with the DHCP client disabled. If your network uses dynamic IP addresses, you must change this setting. To connect to the WAG302 after the DHCP server on your network assigns it a new IP address, enter the wireless access point name into your Web browser. The default wireless access point name is netgearxxxxxx, where xxxxxx represents the last 6 bytes of the MAC address. The default name is printed on the bottom label of the WAG302.

4. Connect the power adapter to the wireless access point and plug the power adapter in to a power outlet. The PWR, LAN, and Wireless LAN lights and should light up.

Verifying Wireless Connectivity

Using a computer with an 802.11b/g or 802.11a wireless adapter with the correct wireless settings needed to connect to the WAG302 (SSID, WEP/WPA, MAC ACL, etc.), verify connectivity by using a browser such as Mozilla Firefox, Netscape or Internet Explorer to browse the Internet, or check for file and printer access on your network.

The default SSID for the 802.11b/g is NETGEAR-11g; the default SSID for the 802.11a is NETGEAR-11a. The SSID of any wireless access adapters must match the SSID configured in the

ProSafe 802.11a/g Dual Band Wireless Access Point WAG302. If they do not match, no wireless connection will be made.

	Note: If you are unable to connect, see Chapter 5, "Troubleshooting."

Logging In Using the Default IP Address

After you install the WAG302, log in to the wireless access point to configure the basic settings and the wireless settings. The WAG302 is set, by default, with the IP address of 192.168.0.230 with DHCP disabled.

	Note: The computer you are using to connect to the WAG302 should be configured with an IP address that starts with 192.168.0.x and a Subnet Mask of 255.255.255.0.

To log in using the default IP Address:

1. Open a Web browser such as Mozilla Firefox, Internet Explorer or Netscape Navigator.
2. Connect to the WAG302 by entering its default address of **http://192.168.0.230** into your browser.

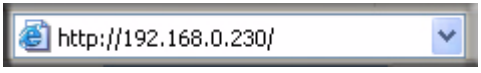


Figure 2-7

3. The login screen will display. Enter **admin** for the user name and **password** for the password, both in lower case letters.

Figure 2-8

4. Click **Login now**.

   Your Web browser should automatically find the WAG302 Wireless Access Point and display the home screen, as shown in Figure 2-8 above.

Setting Basic IP Options

The basic settings for your wireless access point are entered on this screen. With the exception of selecting the correct Country/Region, most of the other default settings will work in most cases. However, if your wireless access point is part of a more complex LAN network, then modify the settings to meet the requirements of your network based on the explanation of the various fields.

To configure the basic settings of your wireless access point:

1. Under Setup on the main menu, select Basic Settings. The Basic Settings screen will display as shown in Figure 2-9 below.

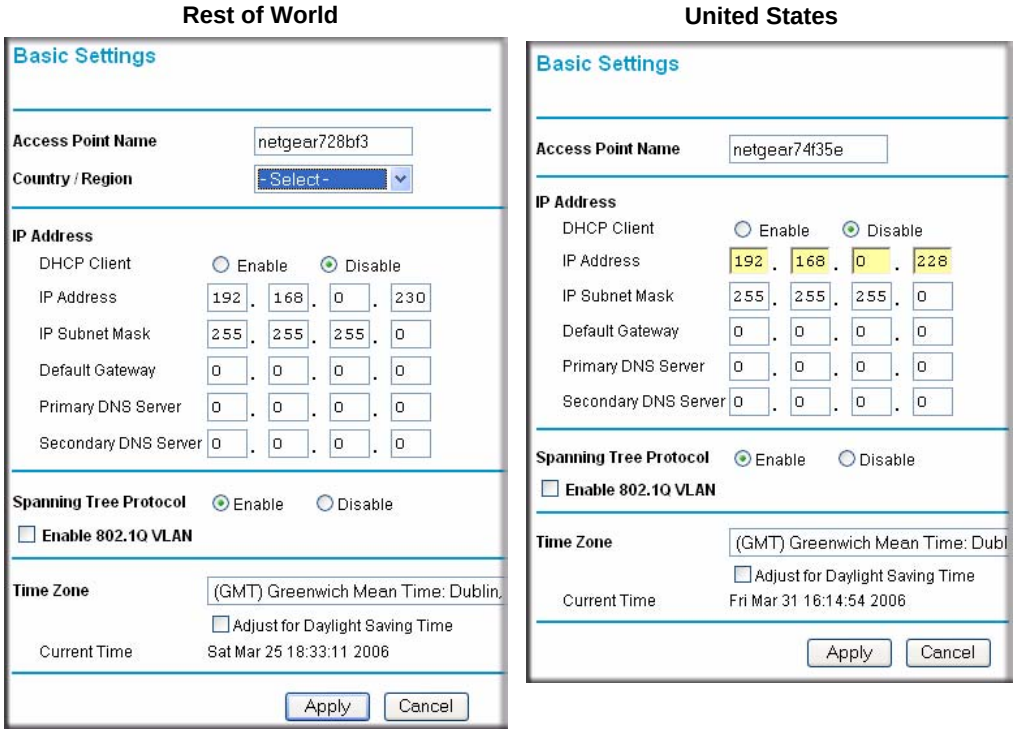


Figure 2-9

2. Enter the **Access Point Name** of the WAG302.

   This unique name is the access point NetBIOS name. The default Access Point Name is located on the bottom label of WAG302. The default is netgearxxxxxx, where xxxxxxx represents the last 6 digits of the WAG302 MAC address. You may modify the default name with a unique name up to 15 characters long.

3. From the **Country/Region** pull-down menu, select the region where the WAG302 can be used (the Country/Region is present in the United States).

	Note: If your country or region is not listed, please check with your local government agency.

4. Enter the IP Address fields of the WAG302.

- **DHCP Client**. By default, the Dynamic Host Configuration Protocol (DHCP) client is disabled. If you have a DHCP server on your LAN and you enable DHCP, the wireless access point will get its IP address, subnet mask and default gateway settings automatically from the DHCP server on your network when you connect the WAG302 to your LAN.
- **IP Address.** Enter the IP Address of your wireless access point.The default IP address is 192.168.0.230. To change it, enter an unused IP address from the address range used on your LAN; or enable DHCP.
- **IP Subnet Mask**. The Access Point will automatically calculate the subnet mask based on the IP address that you assign. Otherwise, you can use 255.255.255.0 (the default) as the subnet mask.
- **Default Gateway.** Enter the IP address of the gateway for your LAN. For more complex networks, enter the address of the router for the network segment to which the wireless access point is connected. The default is 0.0.0.0.
- **Primary DNS Servers.** The WAG302 will use this IP address as the primary Domain Name Server used by stations on your LAN. The default is 0.0.0.0.
- **Secondary DNS Servers.** The WAG302 will use this IP address as the secondary Domain Name Server used by stations on your LAN. The default is 0.0.0.0.

5. **Spanning Tree Protocol.** Enable or disable spanning tree protocol. Spanning tree protocol provides network traffic optimization in settings with multiple WAG302 Wireless Access Points. The default is Enabled.
6. **Enable 802.1Q VLAN.** If enabled, each Security Profile will be associated with the default VLAN for WAG302. (Useful primarily if the hubs/switches on your LAN support the VLAN 802.1Q standard.) The default is Disabled.
7. From the pull-down menu, select the local **Time Zone** for your wireless access point from a list of all available time zones. The default is GMT.
8. Check the **Adjust for Daylight Saving Time** if your location uses daylight saving. The default is no adjustment.

	Note: You must have an Internet connection to get the current time.

9. Click **Apply** to save your Basic IP settings.

Wireless Settings

The following sections describe how to configure the wireless settings available in both the 80211.a and 80211.b/g modes.

Configuring 802.11a Wireless Settings

To configure the 80211.a wireless settings of your wireless access point:

1. From the main menu under Setup, select Wireless Settings 11a. The Wireless Settings 11a screen will display as shown in Figure 2-10 below.

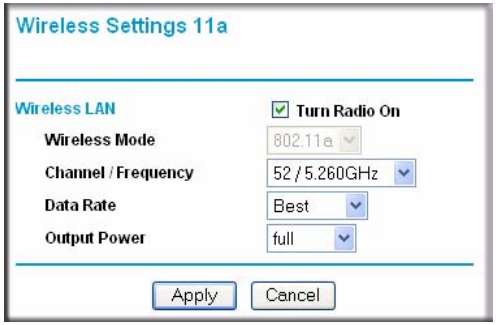


Figure 2-10

2. Configure the Wireless LAN settings based on the following field descriptions:

   - **Turn Radio On**. On by default, you can also turn off the radio to disable access through this device. This can be helpful for configuration, network tuning, or troubleshooting activities.
   - **Wireless Mode**. From the pull-down menu, select the desired wireless operating mode. Only 802.11a wireless stations can be selected from this menu.
   - **Channel/Frequency**. From the pull-down menu, select the channel you wish to use on your wireless LAN. The default is channel 52.

     It should not be necessary to change the wireless channel unless you experience interference (shown by lost connections and/or slow data transfers). Should this happen, you may want to experiment with different channels to see which is the best. See the article on “Wireless Channels” available on the NETGEAR website. (A link to this article and other articles of interest can be found in Appendix B, “Related Documents.”). When selecting or changing channels, some points to bear in mind:

  - Access points use a fixed channel. You can select the channel used. This allows you to choose a channel which provides the least interference and best performance. In the USA and Canada, 13 channels are available.
  - If using multiple access points, it is better if adjacent access points use different channels to reduce interference. The recommended channel spacing between adjacent access points is 8 channels (for example, use channels 36 and 44, or 44 and 52).
  - In "Infrastructure" mode, wireless stations normally scan all channels, looking for an access point. If more than one access point can be used, the one with the strongest signal is used. This can only occur when the various access points are using the same SSID.

- **Data Rate**. From the pull-down menu, select the transmit data rate of the wireless network. The possible data rates supported are: 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps. The default is Best.
- **Output Power**. From the pull-down menu, select the transmit power of the access point. The options are Full, Half, Quarter, Eighth, and Min. Decrease the transmit power if two or more APs are close together and use the same channel frequency. The default is Full. (The transmit power may vary depending on the local regulatory regulations.

3. Click **Apply** to save your 802.11a wireless settings.

Configuring 802.11b/g Wireless Settings

To configure the wireless settings of your 802.11 b/g wireless access point:

1. From main menu under Setup, select Wireless Settings 11b/g. The Wireless Settings 11b/g screen will display as shown in Figure 2-11 below.

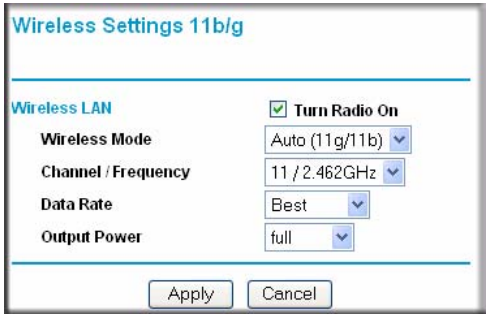


Figure 2-11

2. Configure the Wireless LAN settings based on the following field descriptions:

- **Turn Radio On**. On by default, you can also turn off the radio to disable access through this device. This can be helpful for configuration, network tuning, or troubleshooting activities.
- **Wireless Mode**. From the pull-down menu, select the desired wireless operating mode. The options are:
  - Auto (11g/11b) – Both 802.11g and 802.11b wireless stations can be supported. This is the default.
  - 11g Only – Only 802.11g wireless stations can be used.
  - 11b Only – All 802.11b wireless stations can be used. (The 802.11g wireless stations can still be used if they can operate in 802.11b mode.)
- **Channel/Frequency**. From the pull-down menu, select the channel you wish to use on your wireless LAN. The wireless channel in use will be between 1 to 11 for US and Canada, 1 to 13 for Europe and Australia. The default is channel 11.

  It should not be necessary to change the wireless channel unless you experience interference (shown by lost connections and/or slow data transfers). Should this happen, you may need to experiment with different channels to see which is the best. See the article on "Wireless Channels" available on the NETGEAR website. (A link to this article and other articles of interest can be found in Appendix B, "Related Documents."). When selecting or changing channels, some points to bear in mind:
  - Access points use a fixed channel. You can select the channel used. This allows you to choose a channel which provides the least interference and best performance. In the USA and Canada, 11 channels are available
  - If using multiple access points, it is better if adjacent access points use different channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use channels 1 and 6, or 6 and 11).
  - In "Infrastructure" mode, wireless stations normally scan all channels, looking for an access point. If more than one access point can be used, the one with the strongest signal is used. This can only happen when the various access points are using the same SSID.
- **Data Rate**. From the pull-down menu, select the available transmit data rate of the wireless network. The possible data rates supported are: Best, 1 Mbps, 2 Mbps, 5.5 Mbps, 11 Mbps, 12 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, 54 Mbps and 108 Mbps. The default is Best.

- **Output Power**. From the pull-down menu, select the transmit power of the access point. The options are Full, Half, Quarter, Eighth, and Min. Decrease the transmit power if two or more APs are close together and use the same channel frequency. The default is Full. (The transmit power may vary depending on the local regulatory regulations.

3. Click **Apply** to save your 802.11b/g wireless settings.

Setting Up and Testing Basic Wireless Connectivity

Follow the instructions below to set up and test basic wireless connectivity. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs.

1. From your web browser, log in to the WAG302 using its default address of **http://192.168.0.230**. Use the default user name of **admin** and default password of **password**— or use a new LAN address and password if you have set them up.
2. From the main menu under Setup, select Basic Settings. Verify that the correct Country/ Region in which the wireless interface will operate has been selected.
3. Click **Apply** to save any changes.
4. From the main menu under Setup, select your network—either the Wireless Settings 11a or Wireless Settings 11b/g. Verify that the correct (default) channel has been selected for your network.

   It should not be necessary to change the wireless channel unless you notice interference problems or are near another wireless access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your wireless access point.
5. Click **Apply** to save any changes.
6. From the main menu under Security, select your network Security Profile settings—either Security Profile settings 11a or Security Profile settings 11b/g. For initial configuration and testing, the Security Profile Settings for Profile 1 (the default profile) are set to Open System and the SSID for 11a set to NETGEAR_11a and the SSID for 11b/g set to NETGEAR_11g (see “Understanding Security Profiles” on page 2-18 to configure a profile).

   Note: The SSID of any wireless access point must match the SSID you configured in the WAG302 Wireless Access Point. If they do not match, you will not get a wireless connection to the WAG302.
7. Click **Apply** to save any changes.

8. Configure and test your PCs for wireless connectivity

Program the wireless adapter of your PCs to have the same SSID and channel that you configured in the WAG302. Check that they have a wireless link and are able to obtain an IP address by DHCP from the WAG302.

	Note: If you are configuring the WAG302 from a wireless computer and you change the SSID, channel, or Security Profile settings, you will lose your wireless connection when you click Apply. You must then change the wireless settings of your computer to match the new settings.

Once your PCs have basic wireless connectivity to the WAG302, you can configure the advanced wireless security functions.

Understanding Security Profiles

Security Profiles let you configure unique security settings for each SSID. You can configure up to eight unique 802.11a wireless security profiles or up to eight unique 802.11b/g wireless security profiles on the WG302. The Security Profiles screens are shown below in Figure 2-12.

	Note: If you are using a RADIUS Server, configure the RADIUS settings first, as described in the "Configuring WEP" on page 2-28.

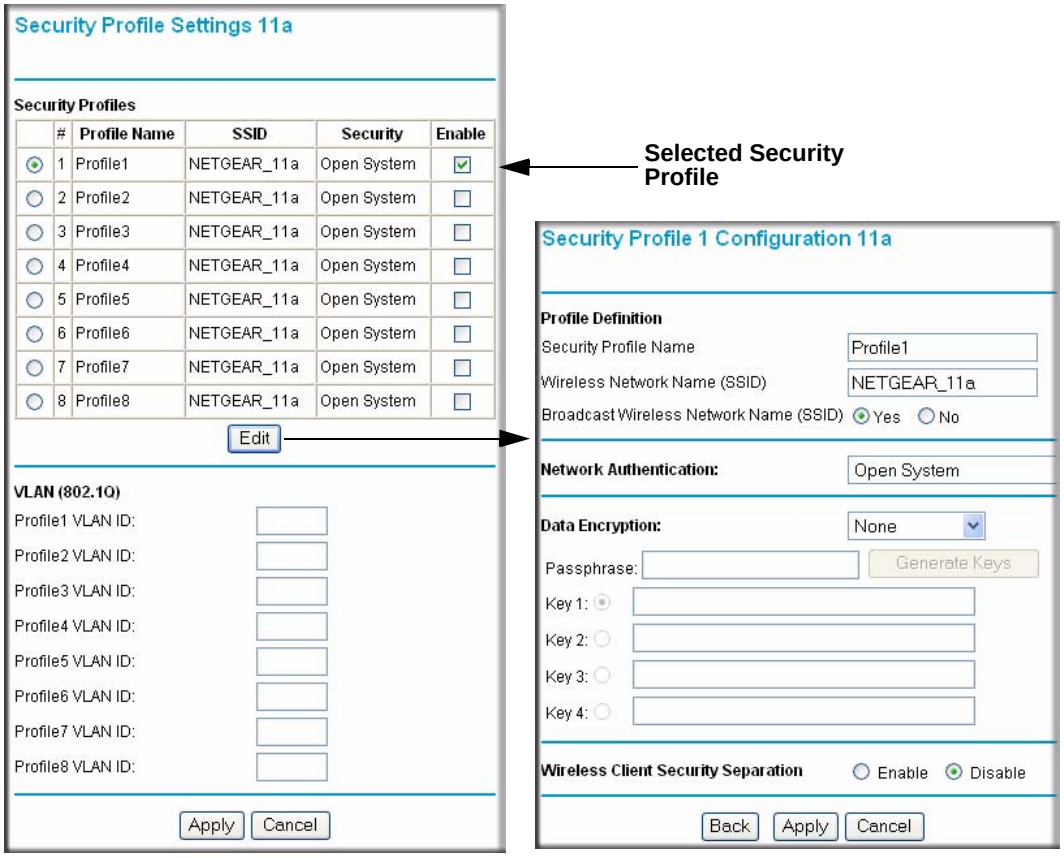


Figure 2-12

An overview of the information that is required to set up a Security Profile follows—including a description of the Network Authentication choices that are available:

- **Security Profile Name**. Use a name that makes it easy to recognize the profile—and to tell profiles apart. (The default names are Profile1, Profile 2, and so on.) You can enter a value of up to 32 alphanumeric characters.

	Note: Only the first profile is enabled by default. The rest of the profiles are disabled and must be enabled if configured.

- **Wireless Network Name (SSID).** This is the name of your wireless network. It is set to the default name of NETGEAR_11a for 802.11a and NETGEAR_11g for 802.11b/g.

- **Network Authentication**. The WAG302 Access Point is set by default as an open system with no authentication. When setting up Network Authentication, bear in mind the following:
  - If you are using Access Point mode, then all options are available. In other modes such as Repeater or Bridge, some options may be unavailable.
  - Not all wireless adapters support WPA or WPA2. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. However, client software is required on the client. Consult the product documentation for your wireless adapter and WPA or WPA2 client software for instructions on configuring WPA2 settings.

  You can configure the WG302v2 to use the types of network authentication shown in the table below.

Table 2-1. Network Authentication Types

Type[a]	Description
Open System	Can be used with WEP encryption or no encryption.
Shared Key	You must use WEP encryption and enter at least one shared key.
Legacy 802.1x	You must configure the RADIUS Server Settings to use this option.
WPA with RADIUS	You must configure the RADIUS Server Settings to use this option.
WPA2 with RADIUS WPA2 is a later version of WPA.	Only select this if all clients support WPA2. If selected, you must use AES encryption and configure the RADIUS Server Settings.
WPA and WPA2 with RADIUS	This selection allows clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, you must use TKIP + AES encryption and configure the RADIUS Server Settings.
WPA-PSK	You must use TKIP encryption and enter the WPA passphrase (Network key).
WPA2-PSKWPA2 is a later version of WPA.	Only select this if all clients support WPA2. If selected, you must use AES encryption and enter the WPA passphrase (Network key).
WPA-PSK and WPA2-PSK	This selection allows clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, you must use TKIP + AES encryption and enter the WPA passphrase (Network key).

a. All options are available if using Access Point mode. In other modes (for example, Repeater or Bridge) some options may be unavailable.

- **Data Encryption**. The available options depend on the Network Authentication setting selected (see Table 2-1 above); otherwise, the default is None. The Data Encryption settings are explained in the table below:

Table 2-2. Data Encryption Settings

Data Encryption Type	Description
None	No encryption is used.
64 bits WEP	Standard WEP encryption, using 40/64 bit encryption.
128 bits WEP	Standard WEP encryption, using 104/128 bit encryption.
152 bits WEP	Proprietary mode that will only work with other wireless devices that support this mode.
TKIP	This is the standard encryption method used with WPA.
AES	This is the standard encryption method for WPA2.
TKIP + AES	This setting supports both WPA and WPA2. Broadcast packets use TKIP. For unicast (point-to-point) transmissions, WPA clients use TKIP, and WPA2 clients use AES.

- Use of Passphrases and Keys are explained below:
  - **Passphrase.** To use the Passphrase to generate the WEP keys, enter a passphrase and click the Generate Keys button. You can also enter the keys directly. These keys must match the other wireless stations.
  - **Key 1, Key 2, Key 3, Key 4**. If using WEP, select the key to be used as the default key. Data transmissions are always encrypted using the default key. The other keys can only be used to decrypt received data.
  - **WPA Preshared Key Passphrase.** If using WPA-PSK, enter the passphrase here. All wireless stations must use the same passphrase (network key). The network key must be from 8 to 63 characters in length.
- **Wireless Client Security Separation**. If enabled, the associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations.) The default is disabled.
- **Profile VLAN ID**. If the hubs/switches on your LAN support the VLAN (802.1Q) standard and this feature has been enabled, the default VLAN ID for WAG302 will be associated with each profile. The default Profile VLAN ID must match the IDs used by other network devices.

SSID and WEP/WPA Settings Setup Form

802.11a Configuration

For a new wireless network, print or copy this form and fill in the configuration parameters. For an existing wireless network, the person who set up or is responsible for the network will be able to provide this information. Be sure to set the Regulatory Domain correctly as the first step.

- **SSID*:*** The Service Set Identification (SSID) identifies the wireless local area network. **NETGEAR_11a** is the default WAG302 SSID. However, you may customize it by using up to 32 alphanumeric characters. Write your customized SSID on the line below.

  _____

  Note: The SSID in the wireless access point is the SSID you configure in the wireless adapter card. All wireless nodes in the same network must be configured with the same SSID:

- **Authentication:**

  Circle one: Open System or Shared Key. (Choose Shared Key for more security.)

  Note: If you select shared key, the other devices in the network will not connect unless they are set to Shared Key as well and have the same keys in the same positions as those in the WAG302.

- **WEP Encryption Keys.**

  Circle one: 64, 128, or 152 bits. (Enter all four 802.11a keys for the Key Size chosen.)

  Key 1: _____

  Key 2: _____

  Key 3: _____

  Key 4: _____

- **WPA-PSK (Preshared Key)**

  Record the WPA-PSK key. Key: _____

- **WPA RADIUS Settings.** For WPA, record the following settings for the primary and secondary RADIUS servers:

  Server Name/IP Address: Primary _____ Secondary _____

  Port: _____

  Shared Secret: _____

802.11b/g Configuration

For a new wireless network, print or copy this form and fill in the configuration parameters. For an existing wireless network, the person who set up or is responsible for the network will be able to provide this information. Be sure to set the Regulatory Domain correctly as the first step.

- **SSID***:* The Service Set Identification (SSID) identifies the wireless local area network. **NETGEAR_11g** is the default WAG302 SSID. However, you may customize it by using up to 32 alphanumeric characters. Write your customized SSID on the line below.

  _____

  Note: The SSID in the wireless access point is the SSID you configure in the wireless adapter card. All wireless nodes in the same network must be configured with the same SSID:

- **Authentication**

  Circle one: Open System or Shared Key. Choose Shared Key for more security.

  Note: If you select shared key, the other devices in the network will not connect unless they are set to Shared Key as well and have the same keys in the same positions as those in the WAG302.

- **WEP Encryption Keys**

  Circle one: 64, 128, or 152 bits. (Enter all four 802.11b/g keys for the Key Size chosen.)

  Key 1: _____

  Key 2: _____

  Key 3: _____

  Key 4: _____

- **WPA-PSK (Preshared Key)**

  Record the WPA-PSK key. Key: _____

- **WPA RADIUS Settings.** For WPA, record the following settings for the primary and secondary RADIUS servers:

  Server Name/IP Address: Primary _____ Secondary _____

  Port: _____

  Shared Secret: _____

Use the procedures described in the following sections to configure the WAG302. Store this information in a safe place.

Configuring the RADIUS Server Settings

You can setup or modify the RADIUS Server settings to compliment Network Authentication security options. The RADIUS Server must be used with Legacy 802.1x, and can be used with WPA and WPA2 Network Authentication. When using a RADIUS Server, the RADIUS Server settings must be configured before completing the Network Authentication security profile (see "Configuring WPA with RADIUS" on page 2-30, "Configuring WPA2 with RADIUS" on page 2-31, or "Configuring WPA and WPA2 with RADIUS" on page 2-32 for specifics on implementing these security options).

Note: The RADIUS Server Settings apply to all profiles. They only need to be configured once per wireless access point.

To set up or modify the RADIUS Server Settings:

1. From your Web browser, log in to the WAG302 using the default LAN address of **http://192.168.0.230**, user name **admin** and password **password**, or use the LAN address and password that you set up.
2. Under Security in the main menu, select RADIUS Server Settings. The radius Server Settings screen will display.
3. Enter the following RADIUS Server settings:
   - **Authentication/Access Control RADIUS Server Login.** This configuration is required for authentication and access control using a RADIUS Server.The IP Address, Port Number and Shared Secret are required for communication with the RADIUS Server. You can configure a Secondary RADIUS Server to use if the Primary RADIUS Server fails.
     - **IP Address.** The IP address of the RADIUS Server. The default is 0.0.0.0.
     - **Port Number.** The port number of the RADIUS Server. The default is 1812.
     - **Shared Secret.** This is shared between the Wireless Access Point and the RADIUS Server while authenticating the supplicant (wireless client).
   - **Reauthentication Time:** The time interval in seconds after which the supplicant will be authenticated again with the RADIUS Server. The default is 3600 seconds.
   - **Global-key Update:** Check this option to update the Global Key. The Global Key can be updated based on time interval in seconds or number of packets exchanged using the global key. The default is 3600 seconds. You can also check the

- **Update if any station disassociates**: Check this radio box to refresh the global key when any stations disassociate from the wireless access point.

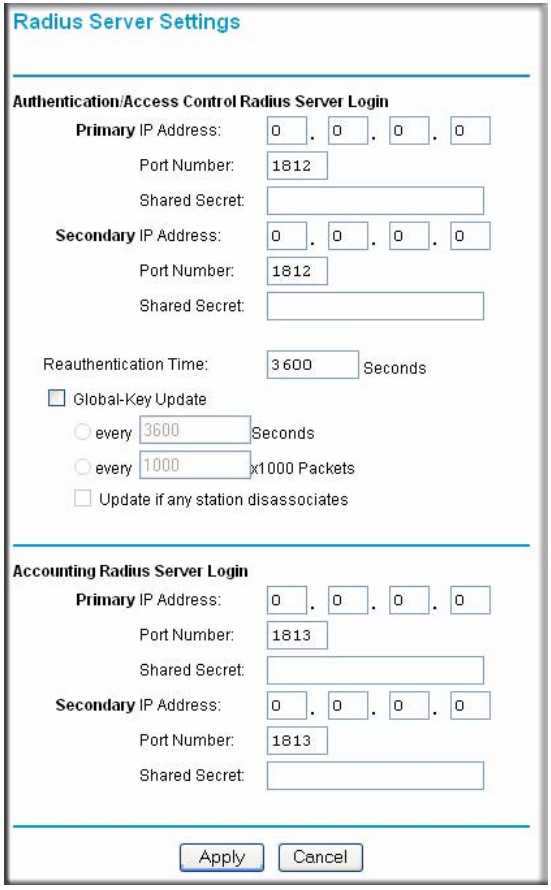


Figure 2-13

- **Accounting Server Configuration**. This configuration is required for accounting using a RADIUS Server. The IP Address, Port Number and Shared Secret are required for communication with the RADIUS Server. You can configure a Secondary RADIUS Server to use if the Primary RADIUS Server fails.
  - **IP Address.** The IP address of the RADIUS Server. The default is 0.0.0.0
  - **Port Number.** Port number of the RADIUS Server. The default: 1813
  - **Shared Secret.** This is shared between the Wireless Access Point and the RADIUS Server while authenticating the supplicant (wireless client).

4. Click **Apply** to save your settings.

Setting up a Security Profile

The WAG302 allows you to set up eight different security profiles for 802.11a and eight different profiles for 802.11b/g. Each profile can be configured with a different security option for network authentication.

Note: If you are using a RADIUS Server, configure the RADIUS settings first, as described in the "Configuring the RADIUS Server Settings" on page 2-24.

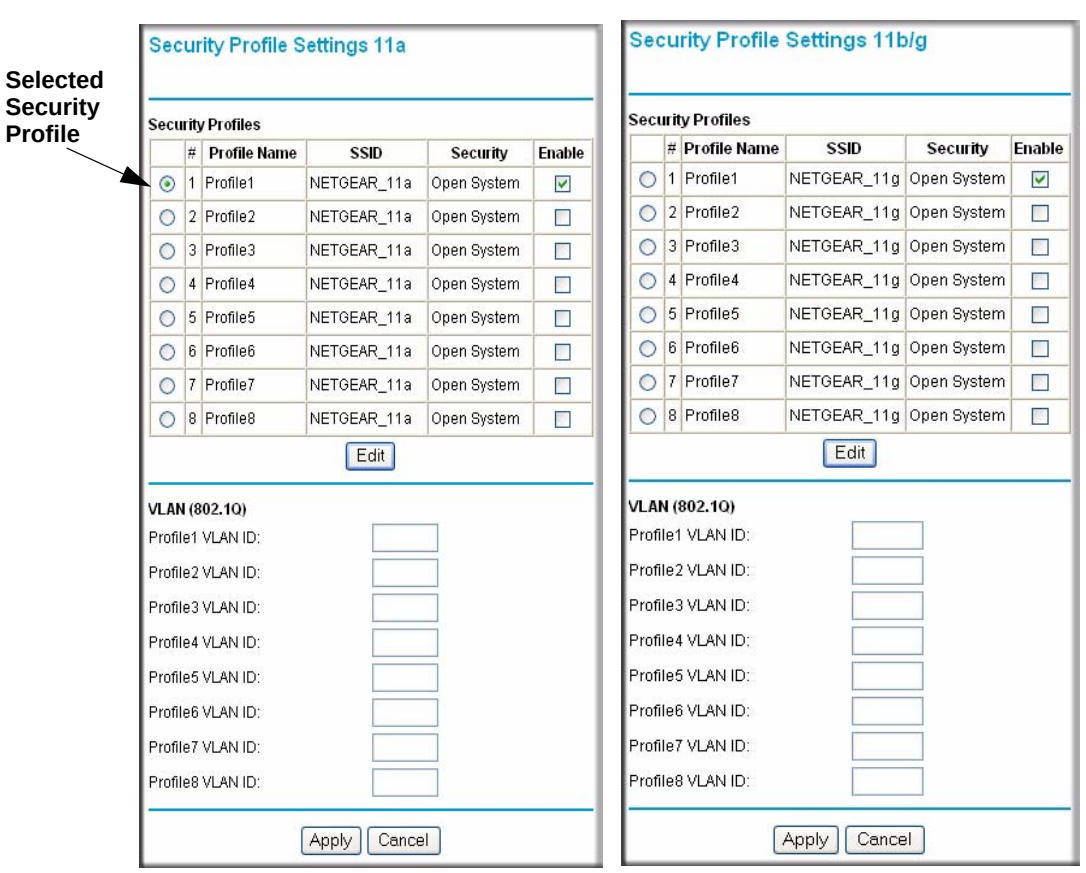


Figure 2-14

To configure a Security Profile:

1. From your Web browser, log in to the WAG302 using the default LAN address of **http://192.168.0.230**, user name **admin** and password **password**, or use the LAN address and password that you set up.
2. From the main menu under Security, select either Security Profile Settings 11a or Security Profile Settings 11b/g. The screen for the Profile Settings you selected will display as shown in Figure 2-14 above.
3. Check the radio button of the profile you want to modify and click **Edit.** The Security Profile Configuration screen for the selected profile will display.

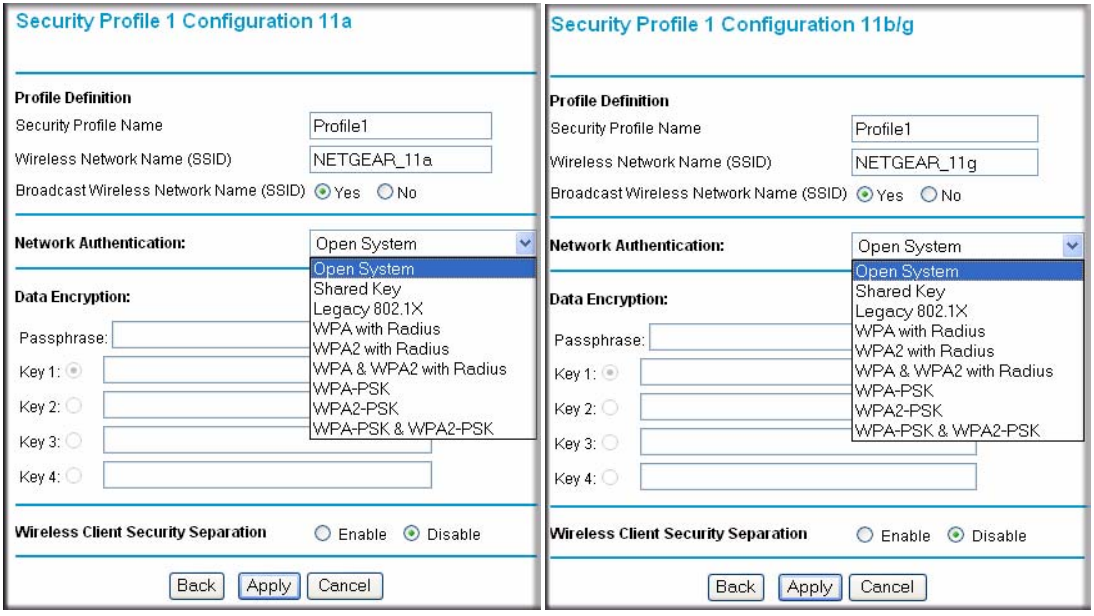


Figure 2-15

4. Give your profile a meaningful name so that you can remember it later.
5. The Wireless Network Name (SSID) is set by default to identify it as either a NETGEAR-11a or a NETGEAR-11g wireless network.
6. Enable or disable the Broadcast Wireless Network Name (SSID). It is enabled by default. (If it is broadcast, it can be easily detected by other clients.)
7. From the pull-down menu shown in Figure 2-15, select the Network Authentication Type you want to use for this profile:

- To configure WEP encryption for Open Systems or Shared Key, see "Configuring WEP" on page 2-28.
- To configure WPA with RADIUS, see "Configuring WPA with RADIUS" on page 2-30.
- To configure WPA2 with RADIUS, see "Configuring WPA2 with RADIUS" on page 2-31.
- To configure WPA and WPA2 with RADIUS, see "Configuring WPA and WPA2 with RADIUS" on page 2-32.
- To configure WPA-PSK, see "Configuring WPA-PSK" on page 2-33.
- To configure WPA2-PSK, see "Configuring WPA2-PSK" on page 2-34.
- To configure WPA-PSK and WPA2-PSK, see "Configuring WPA-PSK and WPA2-PSK" on page 2-35.

8. **Wireless Client Security Separation** is disabled by default. If enabled, the associated wireless clients will not be able to communicate with each other.
9. Click **Apply** to save your Security Profile settings.
10. Click **Back**. Your new settings will appear in the Security Profiles table identified by the Profile Name of the profile. A VLAN ID will also be assigned to your profile.

	Note: Security Profiles that share the same type of network authentication must share the same passphrase or keys. Security Profiles that use WEP must share the same four keys, but they do not need to use the same default key.

To enable your Security Profile:

1. Check the radio box in the **Enable** column next to your profile.
2. Click **Apply**. Your Security Profile will be enabled. If you enabled VLAN 802.1Q, your VLAN Profile will also be enabled. (See "Setting Basic IP Options" on page 2-11 to enable VLAN 802.1Q.)

Configuring WEP

To configure WEP data encryption:

1. From the Network Authentication drop-down menu, choose either Open System or Shared Key authentication.
2. From the Data Encryption drop-down menu, select encryption strength (64 bits, 128 bits, or 152 bits).

3. You manually or automatically program the four data encryption keys. These values must be identical on all PCS and wireless access points in your network. Choose either:
   - Automatic – Enter a word or group of printable characters in the Passphrase box and click the Generate button. The four key boxes will be automatically populated with key values.
   - Manual – Enter the number of hexadecimal digits appropriate to the encryption strength: 10 digits for 64-bit and 26 digits for 128-bit (any combination of 0-9, a-f, or A-F) Select which of the four keys will be the default.

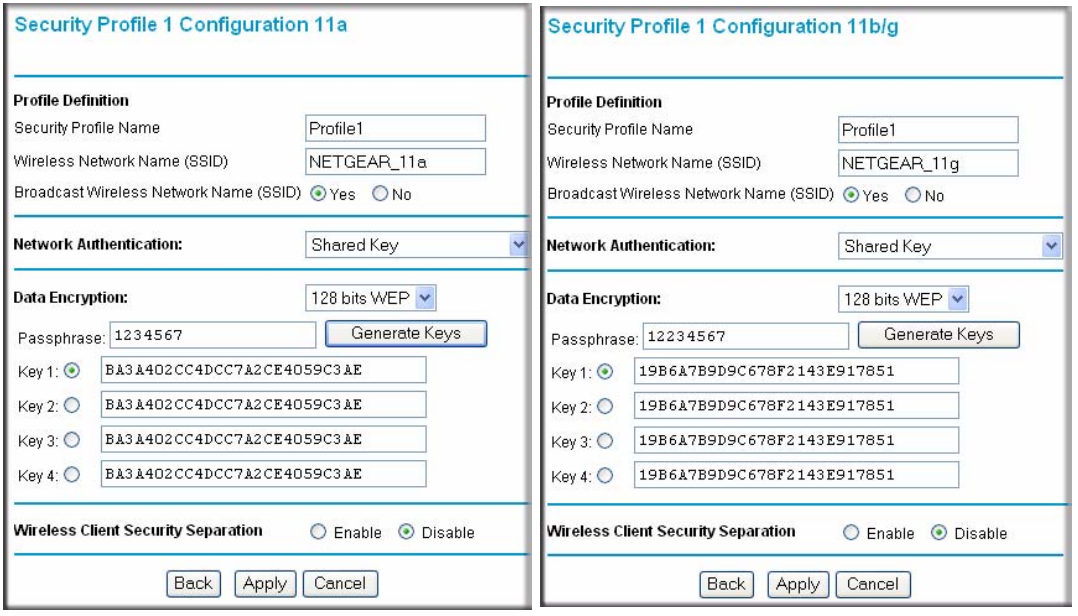


Figure 2-16

4. Select the key to be used as the default key by checking the radio box. (Data transmissions are always encrypted using the default key.)

   See the document "Wireless Communications" for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard. A link to this document on the NETGEAR website is in Appendix B, "Related Documents."

5. **Wireless Client Security Separation** is disabled by default. If enabled, associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations.

6. Click **Apply** to save your settings.

Note: If you use a wireless computer to configure WEP settings, you will be disconnected when you click Apply. Reconfigure your wireless adapter to match the new settings or access the wireless access point from a wired computer to make any further changes.

Configuring WPA with RADIUS

Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 or above do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

To configure WPA, follow these steps:

1. Under Security on the menu, select RADIUS Server Settings. The RADIUS Server Settings screen will display.
2. Enter the RADIUS Server Settings as shown in "Configuring the RADIUS Server Settings" on page 2-24.
3. Click **Apply** to save your RADIUS Server settings.
4. Under Security on the main menu, select either Security Profile Settings 11a or Security Profile Settings 11b/g. When the Security Profile screen displays, check the radio button of the Security Profile you want to modify and click **Edit.**

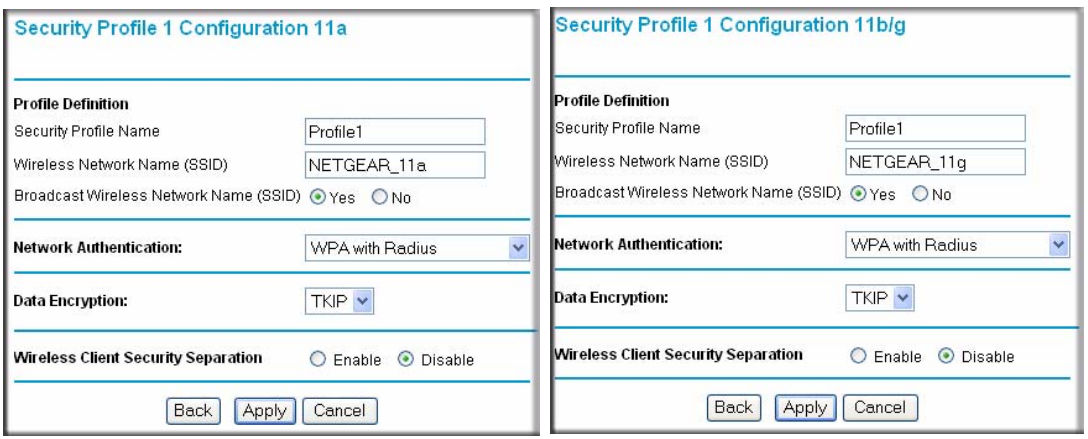


Figure 2-17

5. Choose **WPA with RADIUS** from the from the Network Authentication drop-down menu. Data Encryption will be set to TKIP by default.
6. **Wireless Client Security Separation** is disabled by default. If enabled, associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations.
7. Click **Apply** to save your settings.

Configuring WPA2 with RADIUS

Not all wireless adapters support WPA2. Furthermore, client software is required on the client. Make sure your client card supports WPA2. Consult the product document for your wireless adapter and WPA2 client software for instructions on configuring WPA2 settings.

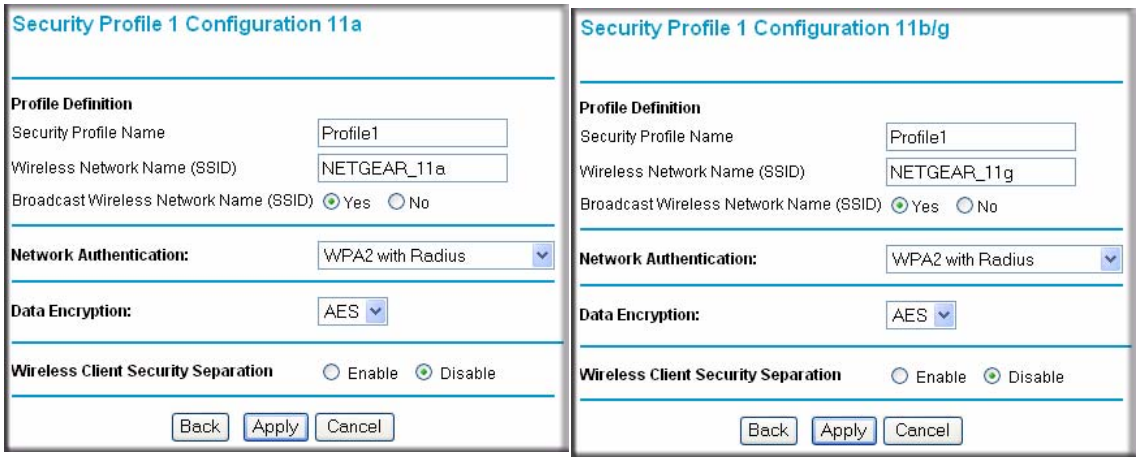


Figure 2-18

To configure WPA2 with RADIUS:

1. Under Security on the main menu, select RADIUS Server Settings. The Select RADIUS Server Settings screen will display.
2. Enter the RADIUS settings as shown in ““Configuring the RADIUS Server Settings” on page 2-24.
3. Click **Apply** to save your RADIUS settings
4. Select Security Profile Settings under Security on the main menu, When the screen displays, check the radio button of the Security Profile you want to modify and click **Edit**.

5. From the Network Authentication drop-down menu, select WPA2 with RADIUS from the list. By default, Data Encryption will be set to AES.
6. **Wireless Client Security Separation** is disabled by default. If enabled, associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations.
7. Click **Apply** to save your settings.

Configuring WPA and WPA2 with RADIUS

Not all wireless adapters support WPA and WPA2. Client software is required on the client:

- Windows XP and Windows 2000 with Service Pack 3, or above, do include the client software that supports WPA. The wireless adapter hardware and driver must also support WPA.
- Service Pack 3 does not include the client software that supports WPA2. Make sure your client card supports WPA2. The wireless adapter hardware and driver must also support WPA2.

Consult the product documentation for your wireless adapter; WPA client software for instructions on configuring WPA settings; and WPA2 client software for instructions on configuring WPA2 settings.

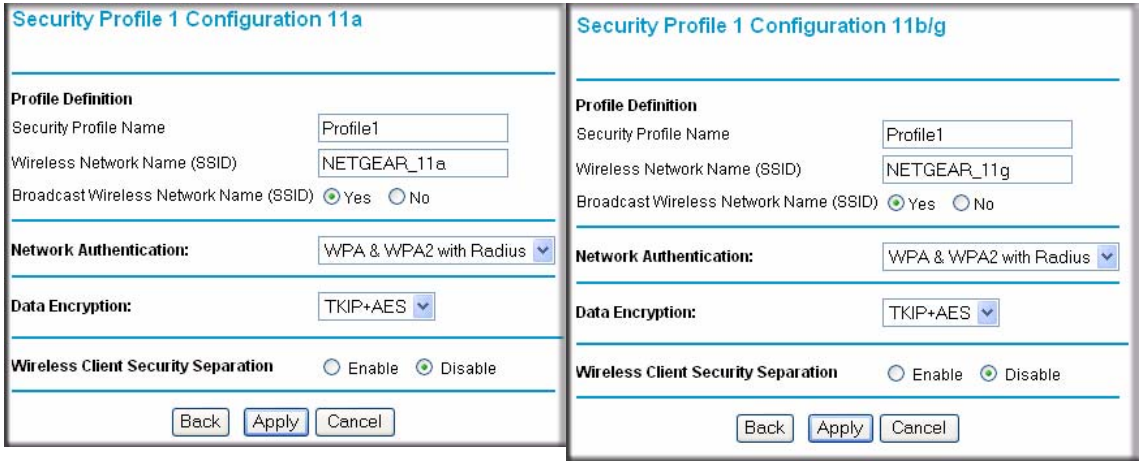


Figure 2-19

To configure WPA and WPA2 with RADIUS:

1. Under Security on the main menu, select RADIUS Server Settings. The Select RADIUS Server Settings screen will display.

2. Enter the RADIUS settings as shown in ""Configuring the RADIUS Server Settings" on page 2-24.
3. Click **Apply** to save your RADIUS settings
4. Select Security Profile Settings under Security on the main menu, When the screen displays, check the radio button of the Security Profile you are modifying and click **Edit**.
5. From the **Network Authentication** drop-down menu, select **WPA & WPA2 with RADIUS** from the list. By default, **Data Encryption** will be set to **TKIP+AES**.
6. **Wireless Client Security Separation** is disabled by default. If enabled, associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations.
7. Click **Apply** to save your settings.

Configuring WPA-PSK

Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 or above include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

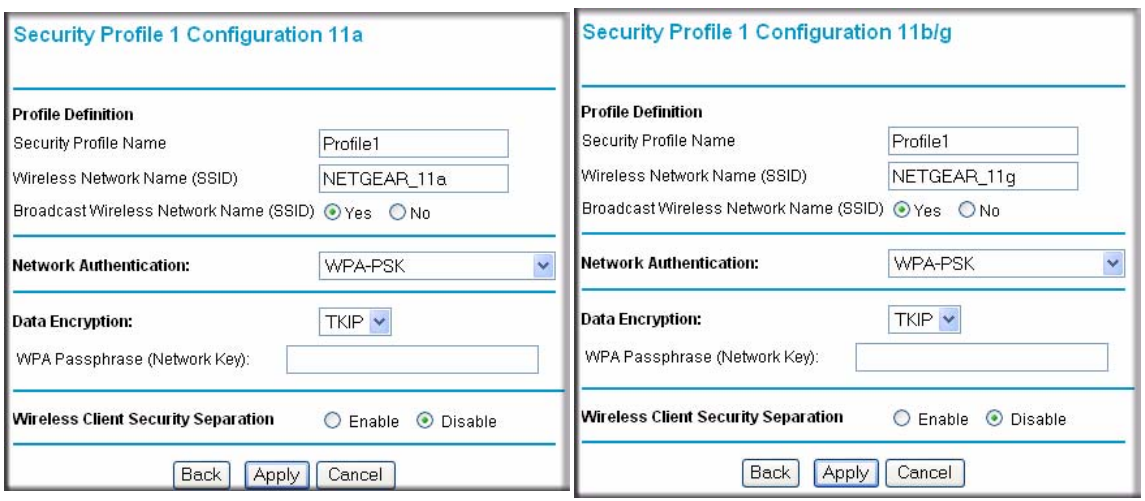


Figure 2-20

To configure WPA-PSK:

1. From the **Network Authentication** drop-down menu, select **WPA-PSK**. By default, **Data Encryption** will be set to **TKIP**.
2. Enter the preshared key passphrase (Network Key).
3. **Wireless Client Security Separation** is disabled by default. If enabled, associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations.
4. Click **Apply** to save your settings.

Configuring WPA2-PSK

Not all wireless adapters support WPA2. Furthermore, client software is required on the client. Make sure your client card supports WPA2. Consult the product document for your wireless adapter and WPA2 client software for instructions on configuring WPA2 settings.

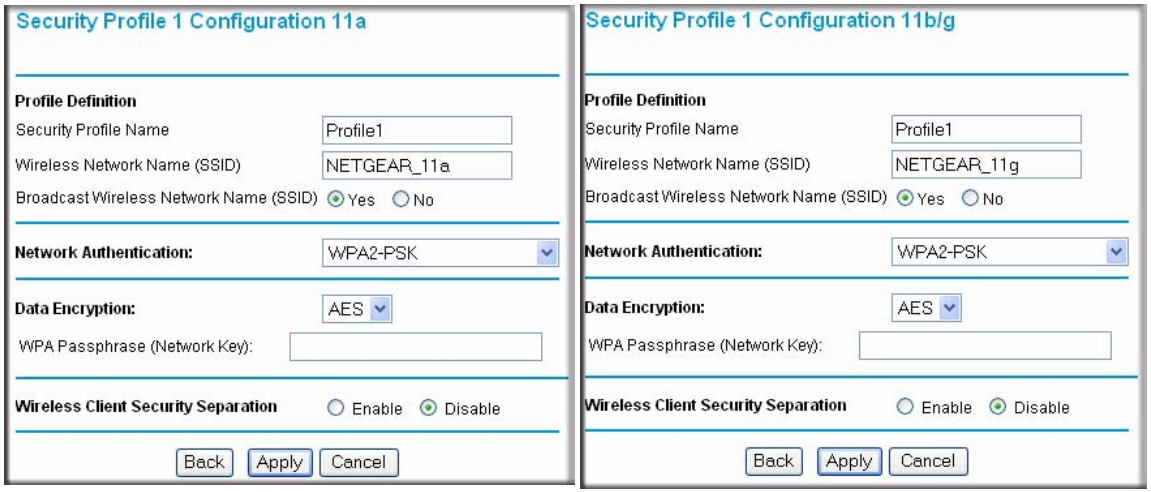


Figure 2-21

To configure WPA2-PSK:

1. From the **Network Authentication** drop-down menu, select **WPA2-PSK** from the list. By default, **Data Encryption** will be set to **AES**.
2. Enter the preshared key passphrase (Network Key).

3. **Wireless Client Security Separation** is disabled by default. If enabled, associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations.
4. Click **Apply** to save your settings.

Configuring WPA-PSK and WPA2-PSK

Not all wireless adapters support WPA and WPA2. Client software is required on the client:

- Windows XP and Windows 2000 with Service Pack 3 or above do include the client software that supports WPA. The wireless adapter hardware and driver must also support WPA.
- Service Pack 3 does not include the client software that supports WPA2. Make sure your client card supports WPA2. The wireless adapter hardware and driver must also support WPA2.

Consult the product documentation for your wireless adapter; WPA client software for instructions on configuring WPA settings; and WPA2 client software for instructions on configuring WPA2 settings.

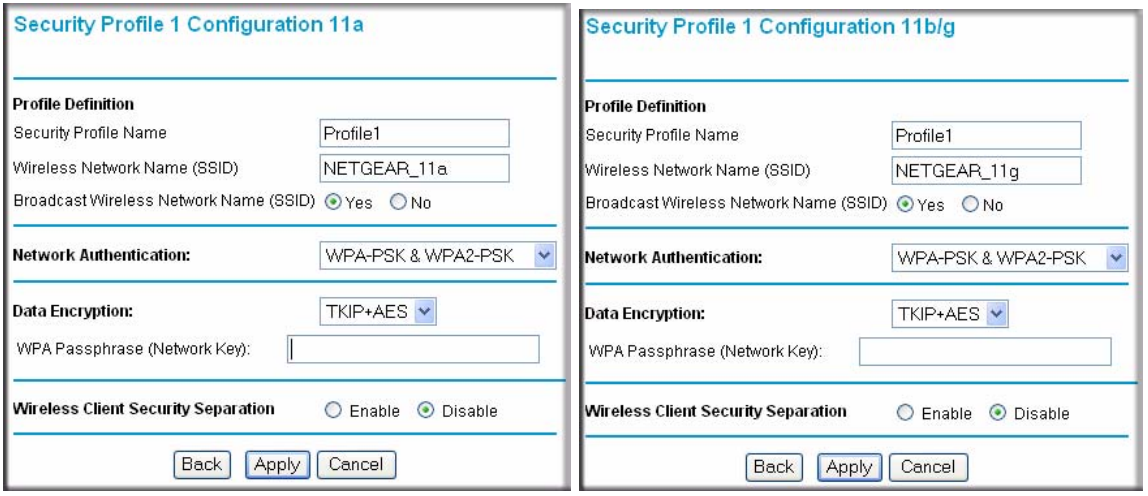


Figure 2-22

To configure WPA-PSK and WPA2-PSK:

1. From the **Network Authentication** drop-down menu, select **WPA-PSK & WPA2-PSK**. By default, **Data Encryption** will be set to **TKIP+AES**.
2. Enter the WPA Passphrase (Network Key).

3. **Wireless Client Security Separation** is disabled by default. If enabled, associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations.
4. Click **Apply** to save your settings.

Restricting Wireless Access by MAC Address

The optional Access Control window lets you block the network access privilege of any specified stations through the WAG302 Wireless Access Point. When you enable access control, the access point only accepts connections from clients on the selected access control list. This provides an additional layer of security.

Note: If configuring the WAG302 from a wireless computer whose MAC address is not in the access control list, if you select Turn Access Control On, you will lose your wireless connection when you click Apply. You must then access the wireless access point from a wired computer or from a wireless computer which is on the access control list to make any further changes.

To restrict access based on MAC addresses:

1. Log in to the WAG302 using the default address of **http://192.168.0.230,** user name of **admin** and default password of **password**, or whatever LAN address and password you have set up.
2. Under Security on the main menu, select and configure Access Control 11a and then select and configure Access Control 11bg. The Access Control screens shown in Figure 2-23 below will display.
3. Check the **Turn Access Control On** radio box to enable Access Control feature.
4. Select the desired Access Control Database options. The options are:
   - Local MAC Address Database – The Access Point will use the local MAC address table for Access Control. This is the default.
   - RADIUS MAC Address Database – The Access Point will use the MAC address table located on the external RADIUS server on the LAN for Access Control. If you choose this database, you must configure the RADIUS Server Settings first (see "Configuring the RADIUS Server Settings" on page 2-24).
5. This list shows any **Trusted Wireless Stations** wireless stations you have entered. If you have not entered any wireless stations this list will be empty. To delete an existing entry, select it and then click **Delete**.

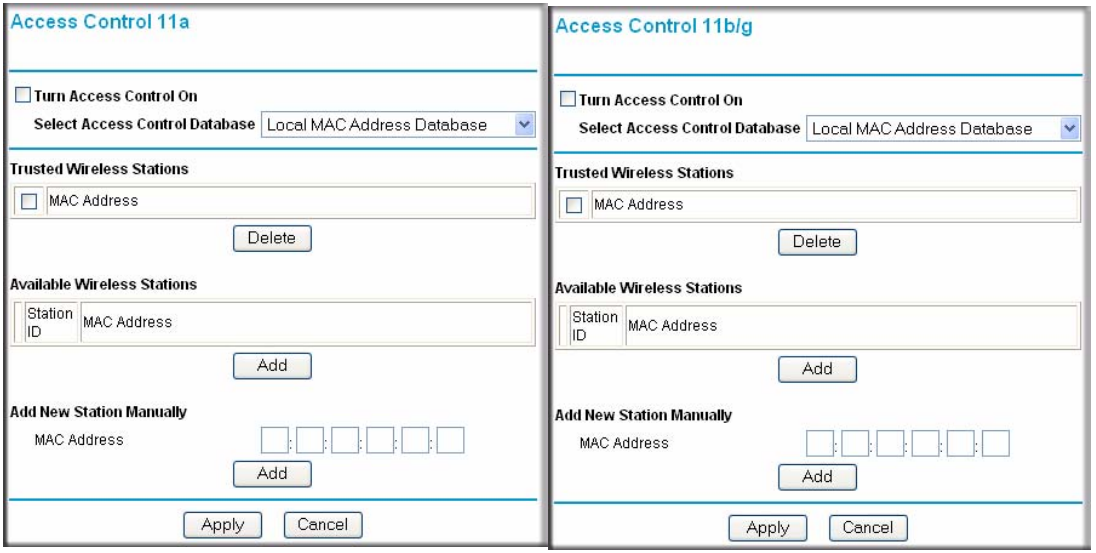


Figure 2-23

6. Select the stations from the list of **Available Wireless Stations** found in your area, or enter the MAC address of a station **Add New Station Manually**. (You can usually find the MAC address printed on the bottom of the wireless adapter.)
7. Click **Add** to add the wireless device to the **Trusted Wireless Stations** list. Repeat these steps for each additional device you want to add to the list.
8. Click **Apply** to save your wireless access control list settings.

Now, only devices on this list will be allowed to wirelessly connect to the WAG302.

Chapter 3
Management

This chapter describes how to use the management features of your ProSafe 802.11a/g Dual Band Wireless Access Point WAG302. To access these features, connect to the WAG302 as described in "Logging In Using the Default IP Address" on page 2-10. Then select the category under either the Management or Information headings in the main menu of the browser interface.

Remote Management

Both the Remote Console and SNMP are enabled by default which allows for remote management of the WAG302 from a from a secure Telnet console as well from a client running SNMP Management software.

To set up a Remote Management interface:

1. Under Management on the main menu, select Remote Management. The Remote Management screen will display.

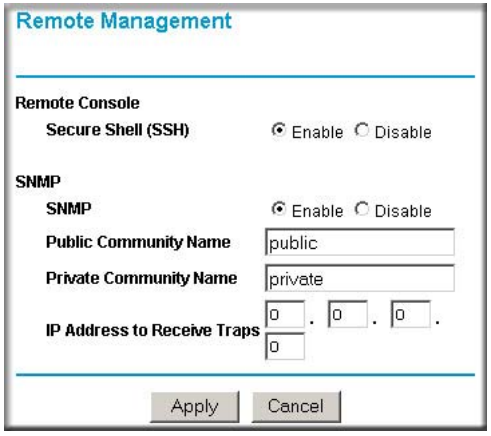


Figure 3-1

2. Enter the following information in the Remote Management fields:

- **Remote Console Secure Shell (SSH):** If set to Enable, the Wireless Access Point will only allow remote access via Secure Shell and Secure Telnet. The default is Enable.
- **SNMP:** Enable SNMP to allow the SNMP network management software, such as HP OpenView, to manage the wireless access point via SNMPv1/v2 protocol.
- **Public Community Name**: The community string to allow the SNMP manager to read the wireless access point's MIB objects. The default is Public.
- **Private Community Name**: The community string to allow the SNMP manager to read and write the wireless access point's MIB objects. The default is Private.
- **IP address to Receive Traps:** The IP address of the SNMP manager to receive traps sent from the wireless access point. The default is 0.0.0.0.

Using the Secure Telnet Interface

The WAG302 includes a secure Telnet command line interface (CLI). You can access the CLI from a secure Telnet client over the Ethernet port or over the serial console port.

Note: You must use a secure Telnet client such as Absolute Telnet. Also, when you configure the client, use the SSH1, 3DES option. If you use the Telnet client to connect over the Ethernet port, use the IP address of the WAG302 as the host name.

To use the CLI from a Console Port:

1. Using the null-modem cable, connect a VT100/ANSI terminal or a workstation to the port labeled Console.

   If you attached a PC, Apple Macintosh, or UNIX workstation, start a secure terminal-emulation program.

2. Configure the terminal-emulation program to use the following settings:
   - Baud rate: 9,600 bps
   - Data bits: 8
   - Parity: none
   - Stop bit: 1
   - Flow control: none

   These settings appear below the connector on the back panel.

3. Press **Return**. The screen shown below in Figure 3-2 should appear.

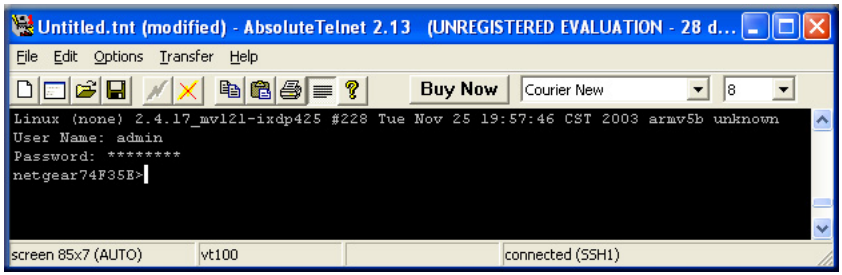


Figure 3-2

4. Enter the login name and password (**admin** and **password** are the defaults).

   After successful login, the <*Access Point Name*> prompt should appear. In this example, the prompt is *netgear74F35E*.

5. Enter `help` to display the CLI command help.

CLI Commands

The CLI commands are listed in Appendix C, “Command Line Reference.”

Using Syslog and Activity Log Information

The Activity Log screen displays the Access Point system activity. It also allows you to enable the SysLog option if you have a SysLog server on your LAN.

To view the Activity Log and enable a SysLog server:

1. From the main menu of the browser interface, under the Information heading, click the Station List link to view the list, shown below.

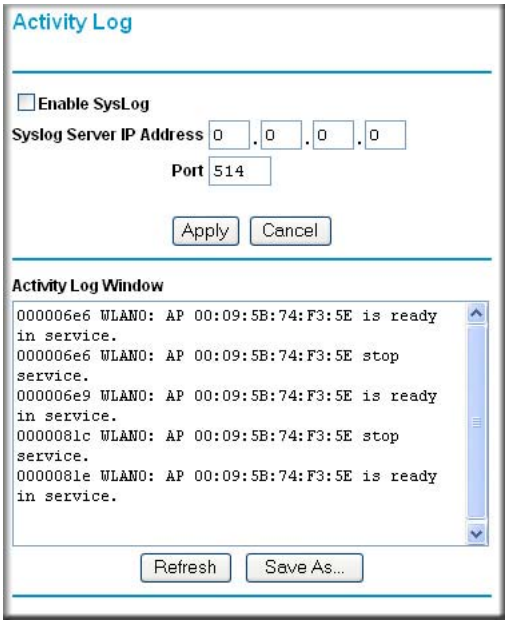


Figure 3-3

2. **Enable SysLog –** Enable this option if you have a SysLog server on your LAN. If enabled, you must enter the IP address of your SysLog server and the port number your SysLog server is configured to use.

   a. **SysLog Server IP address –**The access point will send all the SysLog to the specified IP address if SysLog option is enabled. Default: 0.0.0.0

   b. **Port –** The port number configured in the SysLog server on your LAN. Default: 514

3. Click **Apply** to save your Syslog settings.

The Activity Log Window displays the Access Point system activity.

Click **Refresh** to update the display or click **Save As** to save the log contents into a file on your PC or to save the file to a disk drive.

Viewing General Summary Information

The General information screen provides a summary of the current WAG302 configuration settings, including current IP settings and current Wireless settings. This information is read only, so any changes must be made on other screens.

To access the General screen:

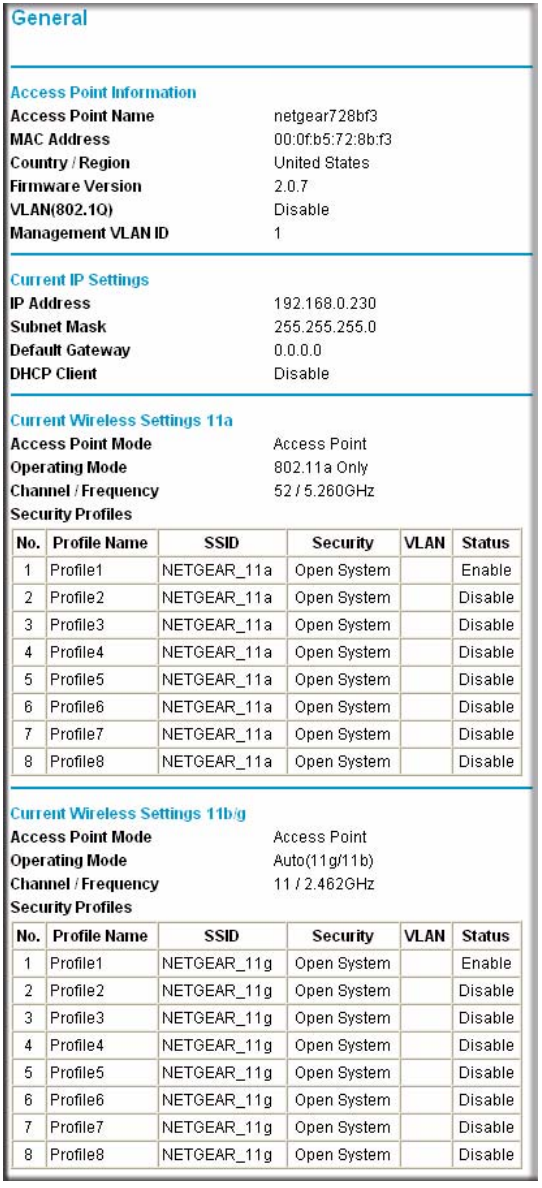
From the main menu of your browser interface, select General to view the General system status screen, shown in Figure 3-4 below. This screen shows the following parameters:

Table 3-1. General Information Fields

Field	Description
Access Point Information	
Access Point Name (NetBIOS name)	The default name may be changed if desired.
MAC Address	Displays the Media Access Control address (MAC address) of the wireless access point's Ethernet port.
Country/Region	Displays the domain or region for which the wireless access point is licensed for use. It may not be legal to operate this wireless access point in a region other than one of those identified in this field.
Firmware Version	The version of the firmware currently installed.
Current IP Settings	
IP Address	The IP address of the wireless access point.
Subnet Mask	The subnet mask for the wireless access point.
Default Gateway	The default gateway for the wireless access point communication.
DHCP Client	Enabled indicates that the current IP address was obtained from a DHCP server on your network. Disabled indicated a static IP configuration.
Current Wireless Settings 11a	
Access Point Mode	Identifies the operating mode of the WAG302: Access Point, Point-to-point bridge, Multi-point bridge or Repeater.
Operating Mode	Identifies the 802.11 operating mode of the WAG302.
Wireless Network Name (SSID)	Displays the wireless network name (SSID) being used by the wireless port of the wireless access point. The default is NETGEAR_11a.
Channel/Frequency	Identifies the channel the wireless port is using. 52 is the default channel setting. (Channel frequencies used on each channel can be found in "Wireless Communications"; a link to this article is in Appendix B, "Related Documents".).

Table 3-1. General Information Fields (continued)

Field	Description
WEP/WPA	WEP/WPA setting.
Current Wireless Settings 11b/g	
Access Point Mode	Identifies the operating mode of the WAG302: Access Point, Point-to-point bridge, Multi-point bridge or Repeater.
Operating Mode	Identifies the 802.11 operating mode of the WAG302.
Wireless Network Name (SSID)	Displays the wireless network name (SSID) being used by the wireless port of the wireless access point. The default is NETGEAR_11g.
Channel/Frequency	Identifies the channel the wireless port is using. 11 is the default channel setting. (Channel frequencies used on each channel can be found in "Wireless Communications"; a link to this article is in Appendix B, "Related Documents".)
WEP/WPA	WEP/WPA setting.



General

Access Point Information

Access Point Name	netgear728bf3
MAC Address	00:0f:b5:72:8b:f3
Country / Region	United States
Firmware Version	2.0.7
VLAN(802.1Q)	Disable
Management VLAN ID	1

Current IP Settings

IP Address	192.168.0.230
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disable

Current Wireless Settings 11a

Access Point Mode	Access Point
Operating Mode	802.11a Only
Channel / Frequency	52 / 5.260GHz

Security Profiles

No.	Profile Name	SSID	Security	VLAN	Status
1	Profile1	NETGEAR_11a	Open System		Enable
2	Profile2	NETGEAR_11a	Open System		Disable
3	Profile3	NETGEAR_11a	Open System		Disable
4	Profile4	NETGEAR_11a	Open System		Disable
5	Profile5	NETGEAR_11a	Open System		Disable
6	Profile6	NETGEAR_11a	Open System		Disable
7	Profile7	NETGEAR_11a	Open System		Disable
8	Profile8	NETGEAR_11a	Open System		Disable

Current Wireless Settings 11b/g

Access Point Mode	Access Point
Operating Mode	Auto(11g/11b)
Channel / Frequency	11 / 2.462GHz

Security Profiles

No.	Profile Name	SSID	Security	VLAN	Status
1	Profile1	NETGEAR_11g	Open System		Enable
2	Profile2	NETGEAR_11g	Open System		Disable
3	Profile3	NETGEAR_11g	Open System		Disable
4	Profile4	NETGEAR_11g	Open System		Disable
5	Profile5	NETGEAR_11g	Open System		Disable
6	Profile6	NETGEAR_11g	Open System		Disable
7	Profile7	NETGEAR_11g	Open System		Disable
8	Profile8	NETGEAR_11g	Open System		Disable

Figure 3-4

Viewing Network Traffic Statistics

The Statistics screen displays information for both wired (LAN) and wireless (WLAN) interface network traffic.

To access Statistics information:

1. Under Information on the main menu, select Statistics. The Statistics screen will display.
2. Click **Refresh** to update the Statistics information. .

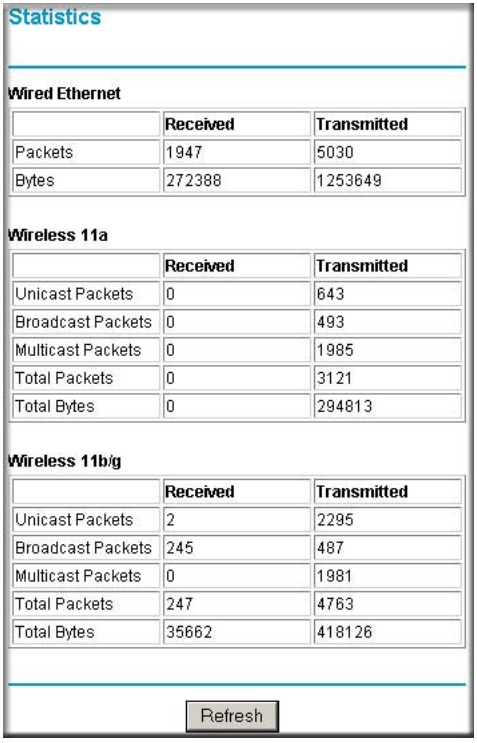


Figure 3-5

Table 3-1, shown below, describes the information fields detailed on the Statistics Screen.

Table 3-1. Statistics Fields

Field	Description
Wired Ethernet	Received/Transmitted
Packets	The number of packets sent since the WAG302 was restarted.
Bytes	The number of bytes sent since the WAG302 was restarted.
Wireless 11a	Received/Transmitted
Unicast Packets	The Unicast packets sent since the WAG302 was restarted.
Broadcast Packets	The Broadcast packets sent since the WAG302 was restarted.
Multicast Packets	The Multicast packets sent since the WAG302 was restarted.
Total Packets	The Wireless packets sent since the WAG302 was restarted.
Total Bytes	The Wireless bytes sent since the WAG302 was restarted.
Wireless 11b/g	Received/Transmitted
Unicast Packets	The Unicast packets sent since the WAG302 was restarted.
Broadcast Packets	The Broadcast packets sent since the WAG302 was restarted.
Multicast Packets	The Multicast packets sent since the WAG302 was restarted.
Total Packets	The Wireless packets sent since the WAG302 was restarted.
Total Bytes	The Wireless bytes sent since the WAG302 was restarted.
Refresh button	Click the Refresh button to update the statistics on this screen.

Viewing Available Wireless Station Statistics

The Available Wireless Station List contains a table of all IP devices associated with this wireless access point in the wireless network defined by the Wireless Network Name (SSID). For each device, the table shows the Station ID, MAC address, IP Address, and Status (whether the device is allowed to communicate with the wireless access point or not).

Note: A wireless network can include multiple wireless access points, all using the same network name (SSID). This enables extending the reach of the wireless network and allows users to roam from one access point to another, providing seamless network connectivity. Under these circumstances, be aware that only the stations associated with this access point will be presented in the Available Station List.

To view the Wireless Station List:

1. From the main menu of the browser interface, under the Information heading, select Available Wireless Station List.

Figure 3-6

2. Click **Refresh** to update the list.

	Tip: If the wireless access point is rebooted, the table data is lost until the wireless access point rediscovers the devices. To force the wireless access point to look for associated devices, click the Refresh button.

Upgrading the Wireless Access Point Software

The software of the WAG302 Wireless Access Point is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR. Upgrade files can be downloaded from Netgear's Web site. If the upgrade file is compressed (.ZIP file), you must first extract the image (.RMT) file before sending it to the wireless access point. The upgrade file can be sent using your browser.

	Note: The Web browser used to upload new firmware into the WAG302 must support HTTP uploads, such as Microsoft Internet Explorer 6.0 or above, or Netscape Navigator 4.78 or above.

You cannot perform the software upgrade from a computer that is connected to the WAG302 Wireless Access Point with a wireless link. You must use a computer that is connected to the WAG302 Wireless Access Point with a Ethernet cable.

	Warning: When uploading software to the WAG302 Wireless Access Point, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, the upload may fail, corrupt the software, and render the WAG302 completely inoperable.

The Web browser used to upload new firmware into the WAG302 must support HTTP uploads, such as Microsoft Internet Explorer 6.0 or above, or Netscape Navigator 4.78 or above.

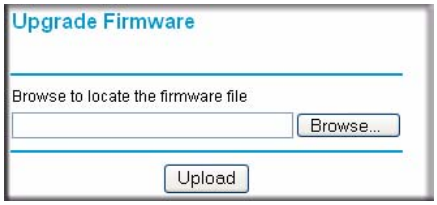


Figure 3-7

To upgrade the WAG302 firmware:

1. Download the new software file from the NETGEAR website, save it to your hard disk, and unzip it.
2. From the main menu under Management, select Upgrade Firmware. The Upgrade Firmware screen will display as shown in Figure 3-7.
3. In the Upgrade Firmware menu, click **Browse** and browse to the location of the image (.RMG) upgrade file.
4. Click **Upload**.

   When the upload completes, your wireless access point will automatically restart. The upgrade process typically takes about 1 minute.

In some cases, you may need to reconfigure the wireless access point after upgrading.

Configuration File Management

The WAG302 Wireless Access Point settings are stored in the wireless access point in a configuration file. This file can be saved (backed up) to a user's computer, retrieved (restored) from the user's computer, or cleared to factory default settings.

To backup or restore your settings:

From the main menu under Management, select Backup/Restore Settings. The Backup/Restore Settings screen will display.

Figure 3-8

The three options displayed are described in the following sections:

Saving and Retrieving the Configuration

The Backup/Restore Settings menu allows you to save or retrieve a file containing your wireless access point's configuration settings.

To save your settings:

1. Click **Save**. Your browser will extract the configuration file from the wireless access point and prompt you for a location on your computer to store the file.
2. Give the file a meaningful name, such as `WAG302.cfg` and click **Save.**

To restore your settings from a saved configuration file:

1. Enter the full path to the file on your computer or click the Browse button to locate the file.
2. When you have located the file, click **Retrieve** to upload the file. After completing the upload, the WAG302 will reboot automatically.

Restoring the WAG302 to the Factory Default Settings

It is sometimes desirable to restore the wireless access point to the factory default settings. This can be done by using the Restore function, which restores all factory settings. After a restore, the wireless access point password will be **password**, the WAG302 DHCP client will be enabled, the default LAN IP address will be 192.168.0.230, and the access point name will reset to the name printed on the label on the bottom of the unit.

To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the wireless access point (see Figure 1-1 on page 1-6). The reset button has two functions:

- **Reboot.** When pressed and released, the Wireless Access Point will reboot (restart).
- **Reset to Factory Defaults.** This button can also be used to clear all data and restore all settings to the factory default values.

To clear all data and restore the factory default values:

1. Power off the WAG302.
2. Use something with a small point, such as a pen, hold the Reset button for 5 seconds while your Power On the WAG302.
3. Continue holding the Reset Button until the LEDs blink twice.
4. Release the Reset Button.

   The factory default configuration has now been restored and the WAG302 is ready for use.

Changing the Administrator Password

The default password is **password**. You should change this password to a more secure password, since you cannot change the administrator login name.

To change the Administrator password:

1. From the main menu of the browser interface, under Management, select Change Password. The Change Password screen will display as shown in Figure 3-9 below.

Figure 3-9

2. First enter the old password in the Current Password field.
3. Then enter the new password twice—once in the New Password field and again in the Repeat New Password field.
4. Click **Apply** to save your change.

Chapter 4
Advanced Configuration

This chapter describes how to configure the advanced features of your ProSafe 802.11a/g Dual Band Wireless Access Point WAG302. The Advanced Configuration features are located under Advanced in the main menu and provide the following functions:

- **IP Settings**. Using the wireless access point as a DHCP server for wireless clients.
- **Hotspot settings.** Enabling HTTP redirect.
- **Wireless Settings**: Configuring advanced wireless LAN parameters.
- **Access Point Settings**: Enabling wireless bridge and repeater modes.

IP Settings for Wireless Clients

You can turn this access point into a DHCP Server for wireless clients for both DHCP-enabled wireless clients as well as for static-IP enabled clients. The default advanced IP wireless settings usually work well. This feature is intended for use by a systems administrator. By default, this feature is not enabled.

To use this wireless access point as a DHCP server:

1. From the main menu under Advanced, select IP Settings. The Advanced IP Settings for Wireless Clients screen will display.
2. Check Use AP as DHCP server and select one of the following options for managing the wireless clients:

   - **Accept DHCP Enabled Wireless Clients Only**: The Access Point can only provide the TCP/IP configurations to those wireless clients with the DHCP enabled.
   - **Accept Both DHCP Enabled and Static IP Configured Wireless Clients**: The Access Point will support wireless clients with the DHCP enabled and the static IP configured.

   The Access Point will provide the preconfigured TCP/IP configurations for all wireless stations connected to this Access Point.

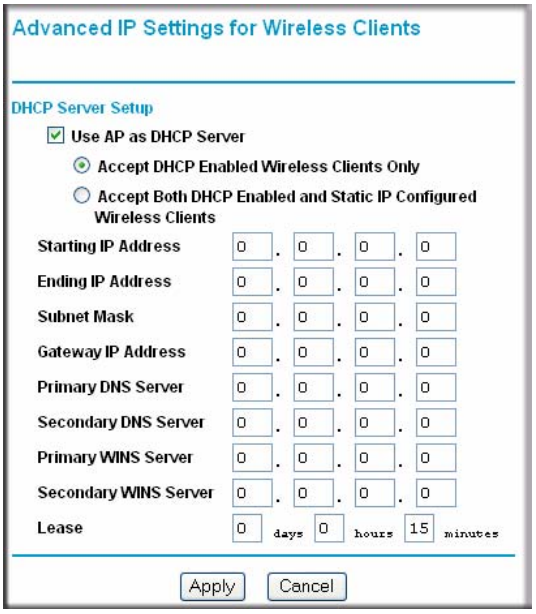


Figure 4-1

3. Configure the following TCP/IP configurations for using theWAG302 as a DHCP Server for wireless clients.

   - **Starting IP Address**: Enter the starting IP address that can be assigned from the DHCP server on this Access Point.
   - **Ending IP Address**: Enter the Ending IP address that can be assigned from the DHCP server on this Access Point
   - **Subnet Mask**: The Access Point will assign the specified subnet mask to the connected wireless stations.
   - **Gateway Address**: The Access Point will assign this IP address as the default gateway for any traffic beyond the local network.
   - **Primary DNS Server**: The Access Point will assign this IP address as the primary Domain Name Server used by the connected wireless stations.
   - **Secondary DNS Serve**r: The Access Point will assign this IP address as the secondary Domain Name Server used by the connected wireless stations.
   - **Primary WINS Server**: The Access Point will assign this IP address as the primary WINS Server used by the connected wireless stations.

- **Secondary WINS Server**: The Access Point will assign this IP address as the secondary WINS Server used by the connected wireless stations.
- **Lease**: The lease time for the IP address assigned. The wireless client user is required to renew the IP address as soon as the lease is expired.

4. Click **Apply** to save your settings.

Hotspot Settings

If you want the wireless access point to capture and redirect all HTTP (TCP, port 80) requests, use this feature to be "captured" and redirected to the specified URL. For example, a hotel might want all wireless connections to go to its server to start a billing transaction.

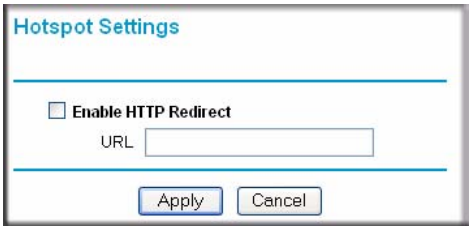


Figure 4-2

To set up a Hotspot server:

1. From the main menu under Advanced, select Hotspot Settings.
2. Check the Enable HTTP Redirect radio button.
3. Enter the URL of the Web server where you wish to redirect HTTP (port 80) requests.
4. Click **Apply**. All port 80 requests will now be redirected to the specified URL.

Configuring Advanced Wireless Settings

The Advanced Wireless Settings screen is used to enable the Wi-Fi Multimedia (WMM) support, and to configure and enable various wireless LAN parameters for both the 11a and 11b/g modes. The default wireless LAN parameters usually work well. However, you can use these settings to fine tune the overall performance of your wireless access point for your environment.

The Advanced Wireless Settings menu is used to configure the following:

- **Wi-Fi Multimedia Support (WMM).** Wireless Multimedia (WMM) is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the type of data. Time-dependent information, such as video or audio, has a higher priority than normal traffic. For WMM to function correctly, Wireless clients must also support WMM.
- **Wireless LAN Parameters.** The default advanced wireless LAN parameter settings usually work well. If you want the wireless access point to operate in SuperA mode (for 11a) or SuperG mode (for 11b/g), use this feature.

To configure Advanced Wireless Settings:

1. From the main menu under Advanced, Select Advanced Wireless Settings 11a or Advanced Wireless Settings 11b/g. The Advanced Wireless Settings screen you selected will display,

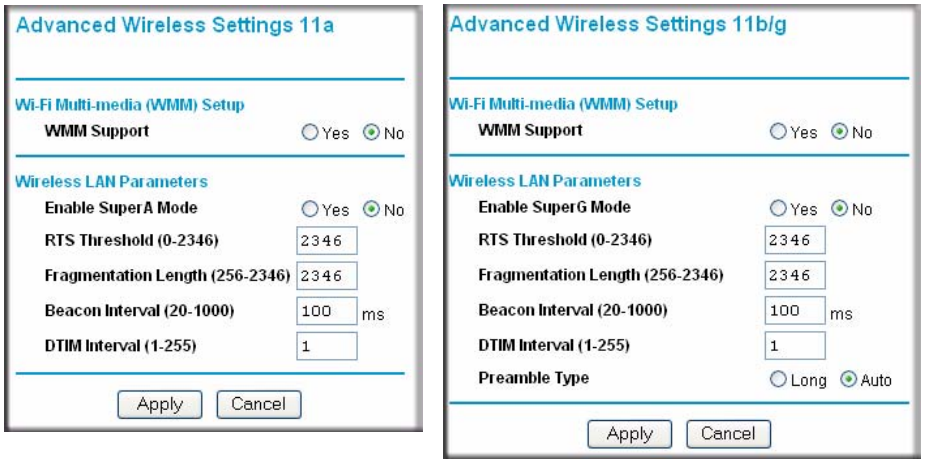


Figure 4-3

2. Wi-FI Multimedia (WMM) is disabled (No) by default. Select the Yes radio button to enable WMM support.

3. Enable the Wireless LAN Parameters by checking the Yes radio button and entering the appropriate information in the fields described below:

- **Enable SuperA or SuperG Mode**: Enable Super-A/G mode may increase the overall wireless performance. The default is disable.

- **RTS Threshold**: Request to Send Threshold. The packet size that is used to determine if it should use the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) mechanism or the CSMA/CA mechanism for packet transmission. With the CSMA/CD transmission mechanism, the transmitting station sends out the actual packet as soon as it has waited for the silence period. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data. The default is 2346.
- **Fragmentation Length**: This is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragment Threshold value must be larger than the RTS Threshold value. The default is 2346.
- **Beacon Interval**: The Beacon Interval. Specifies the interval time between 20ms and 1000ms for each beacon transmission. The default is 100.
- **DTIM Interval**: The Delivery Traffic Indication Message. Specifies the data beacon rate between 1 and 255. The default is 1.
- **Preamble Type (11b/g only):** A long transmit preamble may provide a more reliable connection or a slightly longer range. A short transmit preamble gives better performance. The Auto settings automatically handles both long and short preambles. The default is Auto.

4. Click **Apply** to enable the Advanced Wireless Settings.

Enabling Wireless Bridging and Repeating

The ProSafe 802.11a/g Dual Band Wireless Access Point WAG302 lets you build large bridged wireless networks. Select the desired wireless access point mode for your environment:

- **Wireless Point-to-Point Bridge**. In this mode, the WAG302 will communicate ONLY with another Bridge mode Wireless Station. You must enter the MAC address (physical address) of the other Bridge mode Wireless Station in the field provided. WEP can (and should) be used to protect this communication.
- **Wireless Point-to-Multi-Point Bridge**. Select this only if this WAG302 is the “Master” for a group of Bridge-mode Wireless Stations. The other Bridge-mode Wireless Stations must be set to Point-to-Point Bridge mode, using the MAC address of this WAG302. They then send all traffic to this “Master”, rather than communicate directly with each other. WEP can (and should) be used to protect this traffic.

- **Repeater**. If selected, this wireless access point will operate as a Repeater only, and send all traffic to the remote access point. If selected, you must enter the MAC address (physical address) of the remote access point.

The screens used to configure these options are located by selecting Advanced Access Point Settings 11a or Advanced Access Point Settings 11b/g under Advanced on the main menu (see Figure 4-4 below.

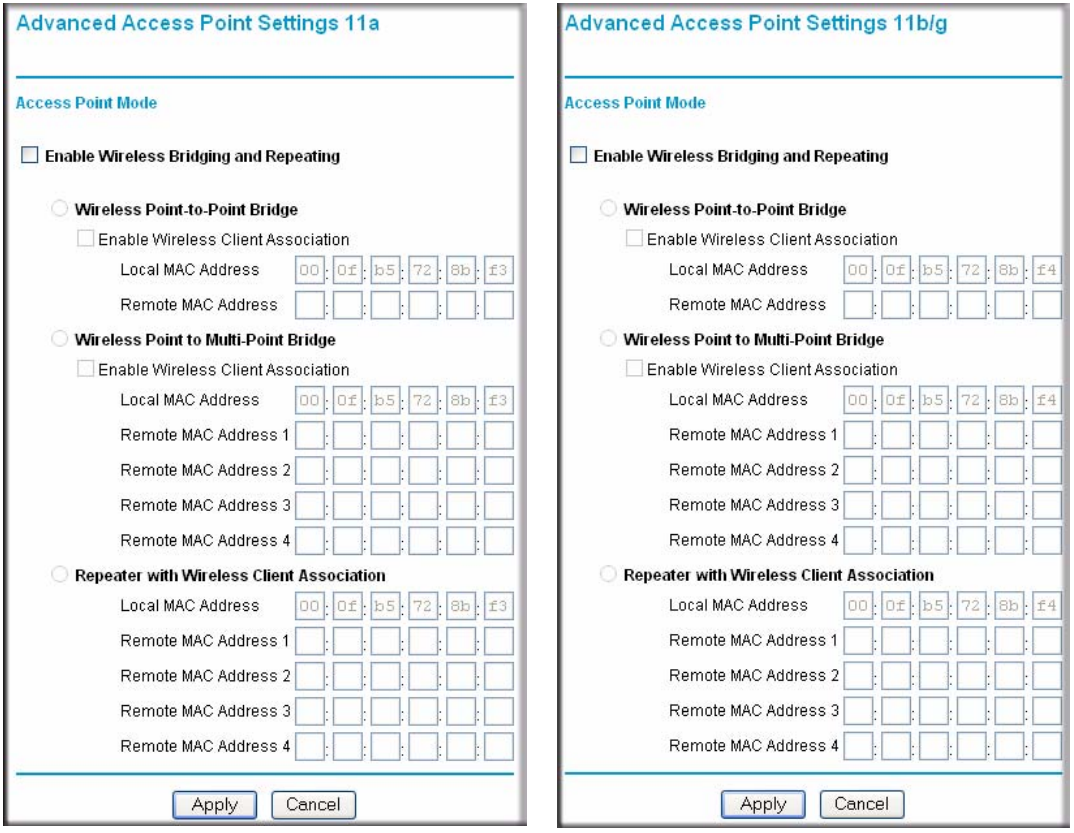


Figure 4-4

The screens used to configure these wireless access point modes are shown in Figure 4-4 above, and described in the following sections.

Configuring a WAG302 as a Point-to-Point Bridge

To configure a point-to-point bridge as shown in Figure 4-5:

1. Under Advanced on the maim menu, select Advanced Access Point Settings 11a or Advanced Access Point Settings 11b/g. The Advanced Access Point Settings screen will display.
2. Configure the WAG302 (AP1) on LAN Segment 1 in Point-to-Point Bridge mode.

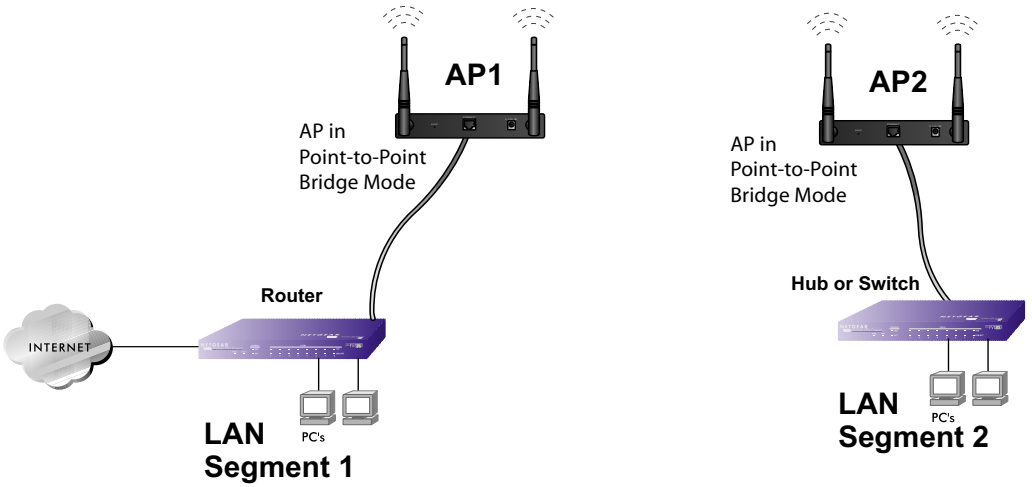


Figure 4-5

3. Configure the WAG302 (AP2) on LAN Segment 2 in Point-to-Point Bridge mode.

   AP1 must have AP2's MAC address in its Remote MAC Address field and AP2 must have AP1's MAC address in its Remote MAC Address field.

4. Configure and verify the following parameters for both access points:

   - Verify that the LAN network configuration of the WAG302 Wireless Access Points both are configured to operate in the same LAN network address range as the LAN devices
   - Both use the same ESSID, Channel, authentication mode, if any, and security settings if security is in use.

5. Verify connectivity across the LAN 1 and LAN 2.

   A computer on either LAN segment should be able to connect to the Internet or share files and printers of any other PCs or servers connected to LAN Segment 1 or LAN Segment 2.

6. Click **Apply** to save your settings.

Configuring a Point-to-Multi-Point Wireless Bridge

To configure a point-to-multi-point wireless bridge as shown in Figure 4-6:

1. Under Advanced on the maim menu, select Advanced Access Point Settings 11a or Advanced Access Point Settings 11b/g. The Advanced Access Point Settings screen will display.

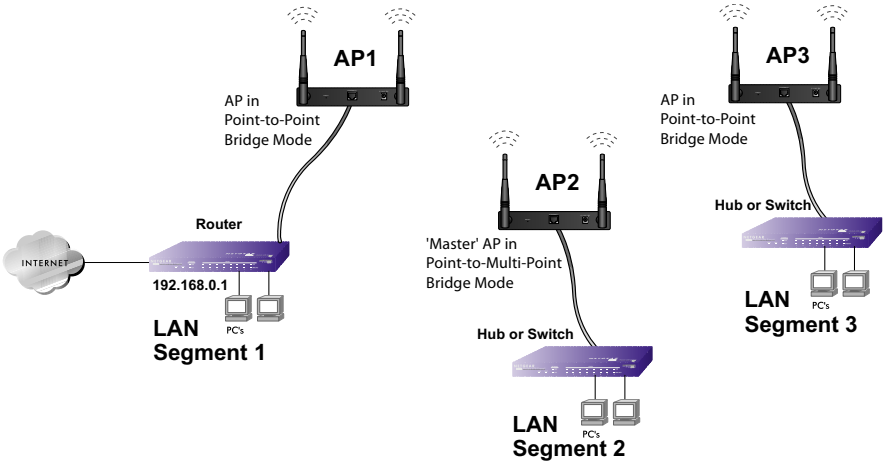


Figure 4-6

2. Configure the Operating Mode of the WAG302 Wireless Access Points.
   - WAG302 (AP1) on LAN Segment 1 in Point-to-Point Bridge mode with the Remote MAC Address of AP2.
   - Because it is in the central location, configure WAG302 (AP2) on LAN Segment 2 in Point-to-Multi-Point Bridge mode. The MAC addresses of the adjacent APs are required in AP2.
   - Configure the WAG302 (AP3) on LAN 3 in Point-to-Point Bridge mode with the Remote MAC Address of AP2.
3. Verify the following parameters for all access points:
   - Verify that the LAN network configuration the WAG302 Wireless Access Points are configured to operate in the same LAN network address range as the LAN devices
   - Only one access point is configured in Point-to-Multi-Point Bridge mode, and all the others are in Point-to-Point Bridge mode.
   - All access points must be on the same LAN. That is, all the APs LAN IP address must be in the same network.

- If using DHCP, all WAG302 Wireless Access Points should be set to “Obtain an IP address automatically (DHCP Client)” in the IP Address Source portion of the Basic IP Settings menu.
- All WAG302 Wireless Access Points use the same SSID, Channel, authentication mode, if any, and encryption in use.
- All Point-to-Point Access Points must have the AP2 MAC address in its Remote AP MAC address field.

4. Verify connectivity across the LANs.

- A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three LAN segments.
- Wireless stations will not be able to connect to the WAG302 Wireless Access Points in the illustration above. If you require wireless stations to access any LAN segment, you can add additional WAG302 Wireless Access Points configured in Wireless Access Point mode to any LAN segment.

5. Click **Apply** to save your settings.

	Note: You can extend this multi-point bridging by adding additional WAG302s configured in Point-to-Point mode for each additional LAN segment. Furthermore, you can extend the range of the wireless network with NETGEAR wireless antenna accessories.

Configuring the WAG302 as a Wireless Repeater

To configure the WAG302 as a Wireless Repeater as shown in Figure 4-7:

1. Under Advanced on the maim menu, select Advanced Access Point Settings 11a or Advanced Access Point Settings 11b/g. The Advanced Access Point Settings screen will display.

2. Configure the Operating Mode of the WAG302 Wireless Access Points.

- WAG302 (AP1) on LAN Segment 1 in Repeater mode with the Remote MAC Address of AP2.
- Configure WAG302 (AP2) in Repeater mode with MAC addresses of AP1 and AP3.

- Configure the WAG302 (AP3) in Repeater mode with the Remote MAC Address of AP2.

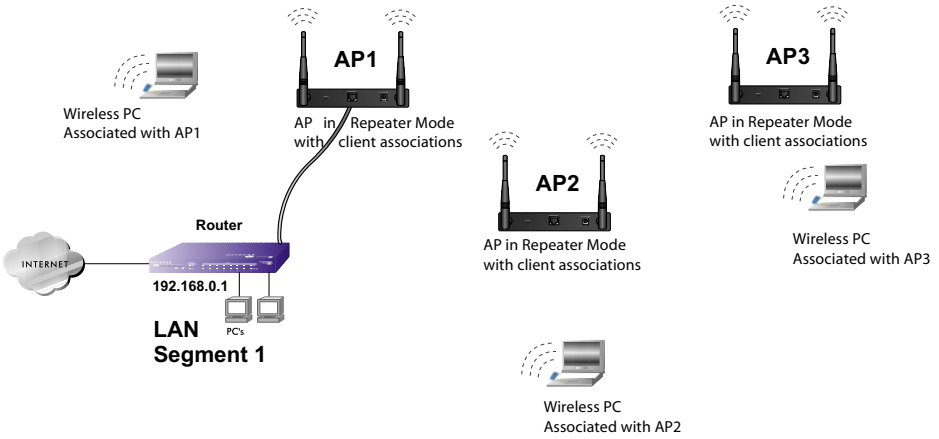


Figure 4-7

3. Verify the following parameters for all access points:

- Verify that the LAN network configuration the WAG302 Wireless Access Points are configured to operate in the same LAN network address range as the LAN devices.
- All access points must be on the same LAN. That is, all the LAN IP addresses of the access points must be in the same network.
- If using DHCP, all WAG302 Wireless Access Points should be set to “Obtain an IP address automatically (DHCP Client)” in the IP Address Source portion of the Basic IP Settings menu.
- All WAG302 Wireless Access Points use the same SSID, Channel, authentication mode, if any, and encryption in use.

4. Verify connectivity across the LANs.

A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three WLAN segments.

5. Click **Apply** to save your settings.

	Note: You can extend repeating by adding up to two additional WAG302s configured in repeater mode. However, since Repeater configurations communicate in half-duplex mode, the bandwidth decreases as you add Repeaters to the network. Also, you can extend the range of the wireless network with NETGEAR wireless antenna accessories.

Chapter 5
Troubleshooting

This chapter provides information about troubleshooting your ProSafe 802.11a/g Dual Band Wireless Access Point WAG302. After each problem description, instructions are given to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the WAG302 on?

  Go to "Installing the WAG302 Wireless Access Point" on page 2-3

- Have I connected the wireless access point correctly?

  Go to "Installing the WAG302 Wireless Access Point" on page 2-3.

- I cannot remember the wireless access point's configuration password.

  Go to "Changing the Administrator Password" on page 3-13.

Note: For up-to-date WAG302 installation details and troubleshooting guidance visit *http://kbserver.netgear.com/products/WG302.asp*.

If you have trouble setting up your WAG302, check the tips below.

No lights are lit on the wireless access point.

It takes a few seconds for the power indicator to light up. Wait a minute and check the power light status on the access point.

If the access point has no power.

- Make sure the power cord is connected to the access point.
- Make sure the power adapter is connected to a functioning power outlet. If it is in a power strip, make sure the power strip is turned on. If it is plugged directly into the wall, verify that it is not a switched outlet.
- Make sure you are using the correct NETGEAR power adapter supplied with your access point.

The Wireless LAN activity light does not light up.

The access point antennas are not working.

- If the Wireless LAN activity light stays off, disconnect the adapter from its power source and then plug it in again.
- Make sure the antennas are tightly connected to the WAG302.
- Contact NETGEAR technical support if the Wireless LAN activity light remains off.

The LAN light is not lit.

There is a hardware connection problem.Check these items:

- Make sure the cable connectors are securely plugged in at the access point and the network device (hub, switch, or router). A switch, hub, or router must be installed between the access point and the Ethernet LAN or broadband modem.
- Make sure the connected device is turned on.
- Be sure the correct cable is used. Use a standard Category 5 Ethernet patch cable. If the network device has Auto Uplink™ (MDI/MDIX) ports, you can use either a crossover cable or a normal patch cable.

I cannot access the Internet or the LAN with a wireless capable computer.

There is a configuration problem. Check these items:

- You may not have restarted the computer with the wireless adapter to have TCP/IP changes take effect. Restart the computer.
- The computer with the wireless adapter may not have the correct TCP/IP settings to communicate with the network. Restart the computer and check that TCP/IP is set up properly for that network. The usual setting for Windows the Network Properties is set to “Obtain an IP address automatically.”
- The access point’s default values may not work with your network. Check the access point default configuration against the configuration of other devices in your network.

I cannot connect to the WAG302 to configure it.

Check these items:

- The WAG302 is properly installed, LAN connections are OK, and it is powered on. Check that the LAN port LED is green to verify that the Ethernet connection is OK.
- The default configuration of the WAG302 is for a static IP address of 192.168.0.230 and a Mask of 255.255.255.0 with DHCP disabled. Make sure your network configuration settings are correct.
- If you are using the NetBIOS name of the WAG302 to connect, ensure that your computer and the WAG302 are on the same network segment or that there is a WINS server on your network.
- If your computer is set to “Obtain an IP Address automatically” (DHCP client), restart it.
- If your computer uses a Fixed (Static) IP address, ensure that it is using an IP Address in the range of the WAG302. The WAG302 default IP Address is 192.168.0.230 and the default Subnet Mask is 255.255.255.0. If you are not sure about these settings, follow the instructions for “Installing the WAG302 Wireless Access Point” on page 2-3.

When I enter a URL or IP address I get a timeout error.

A number of things could be causing this. Try the following troubleshooting steps.

- Check whether other PCs work. If they do, ensure that your PCs TCP/IP settings are correct. If using a Fixed (Static) IP Address, check the Subnet Mask, Default Gateway, DNS, and IP Addresses.
- If the PCs are configured correctly, but still not working, ensure that the WAG302 is connected and turned on. Connect to it and check its settings. If you cannot connect to it, check the LAN and power connections.
- If the WAG302 is configured correctly, check your Internet connection (DSL/Cable modem etc.) to make sure that it is working correctly.
- Try again.

Using the Reset Button to Restore Factory Default Settings

The Reset button (see "Rear Panel" on page 1-8) has two functions:

- **Reboot.** When pressed and released quickly, the WAG302 will reboot (restart).
- **Reset to Factory Defaults.** This button can also be used to clear ALL data and restore ALL settings to the factory default values.

To clear all data and restore the factory default values:

1. Power off the WAG302 and power it back on.
2. Use something with a small point, such as a pen, to press the Reset button in and hold it in for at least 5 seconds.
3. Release the Reset button.

The factory default configuration has now been restored, and the WAG302 is ready for use.

Appendix A
Default Settings and Technical Specifications

This appendix provides the factory default settings and technical specifications for the ProSafe 802.11a/g Dual Band Wireless Access Point WAG302.

Factory Default Settings

You can use the reset button located on the front of your device to reset all settings to their factory defaults. This is called a hard reset.

- To perform a hard reset, push and hold the reset button for approximately 5 seconds (until the TEST LED blinks rapidly). Your device will return to the factory configuration settings shown in Table A-1 below.
- Pressing the reset button for a shorter period of time will simply cause your device to reboot.

Table A-1. Access Point Default Configuration Settings

Feature		Description
AP Login		
	User Login URL	192.168.0.230
	User Name (case sensitive)	admin
	Login Password (case sensitive)	password
Ethernet Connection		
	Static IP Address	192.168.0.210
	Ethernet MAC Address	See bottom label.
	Port Speed	10/100
Local Network (LAN)		
	Lan IP	192.168.0.230
	Subnet Mask	255.255.255.0
	Gateway Address	0.0.0.0
	DHCP Server	Disabled

Table A-1. Access Point Default Configuration Settings

Feature		Description
	DHCP Client	Disabled
	Time Zone	GMT
	Time Zone Adjusted for Daylight Saving Time	Disabled
	SNMP	Enabled, but Trap forwarding disabled
	Spanning Tree Protocol	Enabled
	Secure Telnet	Enabled
Wireless		
	Operating Mode	Access Point
	Access Point Name	netgearxxxxxx where xxxxxx are the last 6 digits of the wireless access point MAC address.
	Wireless Communication	Enabled
	11a Wireless Network Name (SSID)	NETGEAR_11a
	11 b/g Wireless Network Name (SSID)	NETGEAR_11b/g
	Broadcast Network Name SSID	Enabled
	Security	Disabled
	Transmission Speed	Auto[a]
	Country/Region	United States (in North America; otherwise, varies by region)
	80211.a Radio Frequency Channel	52
	80211.g Radio Frequency Channel	11 until the region is selected
	VLAN(802.1Q)	Disabled
	Output Power	Full
	Wireless Card Access List	All wireless stations allowed
	WMM Support	Disabled
	SuperG Mode	Disabled

a. Maximum Wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

Technical Specifications

Table A-2. WAG302 Technical Specifications

Parameter	ProSafe 802.11a/g Dual Band Wireless Access Point WAG302
802.11a Data Rates	6, 9, 12, 18, 24, 36, 48, 54, and 108 Mbps (Auto-rate capable)
802.11a Operating Frequencies	5.15 ~ 5.25 5.25 ~ 5.35 5.57 ~ 5.825
802.11a Encryption	40-bits (also called 64-bits), 128- and 152-bits WEP data encryption
802.11g Data Rates	1, 2, 5.5, 11, 12, 18, 24, 36, 38, 54, & 108 Mbps (Auto-rate capable)
802.11g Operating Frequencies	2.412 ~ 2.462 GHz (US) 2.457 ~ 2.462 GHz (Spain) 2.412 ~ 2.484 GHz (Japan) 2.457 ~ 2.472 GHz (France) 2.412 ~ 2.472 GHz (Europe ETSI)
802.11g Encryption	40-bits (also called 64-bits), 128- and 152-bits WEP data encryption
Network Management	Web-based configuration and status monitoring
Maximum Clients	Limited by the amount of wireless network traffic generated by each node; typically 15 to 20 nodes.
Status LEDs	Power/Ethernet LAN/Wireless LAN/Test
Power Adapter	12V DC, 1.2 A
Electromagnetic Compliance	FCC Part 15 Class B and Class E, CE, and C-TICK
Environmental Specifications	Operating temperature: 0 to 50° C Operating humidity: 5-95%, non-condensing

Appendix B
Related Documents

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document	Link
Internet Networking and TCP/IP Addressing	*http://documentation.netgear.com/reference/enu/tcpip/index.htm*
Wireless Communications	*http://documentation.netgear.com/reference/enu/wireless/index.htm*
Preparing a Computer for Network Access	*http://documentation.netgear.com/reference/enu/wsdhcp/index.htm*
Glossary	*http://documentation.netgear.com/reference/enu/glossary/index.htm*

Appendix C
Command Line Reference

The ProSafe 802.11a/g Dual Band Wireless Access Point WAG302 (AP) can be configured either through the command line interface (CLI), a Web browser, or an MIB browser. The CLI allows viewing and modification of the configuration from a terminal or PC through a telnet connection.

Command Sets

```
get set del keyword                  Description
--- --- --- ---------------------- -------------------------------
[X] [X]     time                   --time setting
[X]           |-now                --current system time
[X] [X]       |-zone               --time zone
[X] [X]       `-daylight saving    --daylight saving
[X] [X]     system                 --system setting
[X]           |-version            --system firmware version
[X] [X]       |-apname             --system name
[X]           |-macaddr            --system MAC address
[X] [X]       |-country            --country/region
[X] [X]       |-dhcpclient         --system dhcp client
[X] [X]       |-ipaddr             --system IP address
[X] [X]       |-netmask            --system network mask
[X] [X]       |-gateway            --system gateway
[X] [X]       |-dns                --system dns
[X] [X]       | |-primary          --primary system DNS server
[X] [X]       | `-secondary        --secondary system DNS server
[X] [X]       |-stp                --enable spanning tree protocol
[X] [X]       |-vlan               --system vlan
[X] [X]       | |-mode             --on/off vlan function
[X]           | `-manage id        --vlan management id
[X]           `-ethstats           --ethernet statistics
[X] [X]     dhcp server            --DHCP server
[X] [X]       |-dhcpserver         --enable DHCP server
[X] [X]       |-anyip              --accept static IP (AnyIP function)
[X] [X]       |-ipstart            --starting IP address
[X] [X]       |-ipend              --ending IP address
[X] [X]       |-netmask            --network mask
[X] [X]       |-gateway            --gateway
[X] [X]       |-dns                --
```

```
get set del keyword                  Description
--- --- --- ---------------------- --------------------------------
[X] [X]       | |-primary          --primary DNS server
[X] [X]       | `-secondary        --secondary DNS server
[X] [X]       |-wins               --
[X] [X]       | |-primary          --primary WINS server
[X] [X]       | `-secondary        --secondary WINS server
[X] [X]       `-lease              --lease time
[X] [X]     radius                 --radius setting
[X] [X]       |-auth               --authenication radius setting
[X] [X]       | |-primary          --primary
[X] [X]       | | |-ipaddr         --radius IP address
[X] [X]       | | |-port           --radius port number
[X] [X]       | | `-secret         --radius secret string
[X] [X]       | `-secondary        --secondary
[X] [X]       |   |-ipaddr         --radius IP address
[X] [X]       |   |-port           --radius port number
[X] [X]       |   `-secret         --radius secret string
[X] [X]       |-account            --account radius setting
[X] [X]       | |-primary          --primary
[X] [X]       | | |-ipaddr         --radius IP address
[X] [X]       | | |-port           --radius port number
[X] [X]       | | `-secret         --radius secret string
[X] [X]       | `-secondary        --secondary
[X] [X]       |   |-ipaddr         --radius IP address
[X] [X]       |   |-port           --radius port number
[X] [X]       |   `-secret         --radius secret string
[X] [X] [X]   `-wpa                --wireless WPA setting
[X] [X]         |-reauthtime       --wireless WPA re-auth period (in seconds)
[X] [X]         `-keyupdate        --enable wireless WPA global key update
[X] [X]           |-mode           --wireless WPA global key update condition
[X] [X]           `-interval       --wireless WPA global key update interval
[X] [X]             |-sec          --wireless WPA global key update interval
                    |                   (in seconds)
[X] [X]             `-pkt          --wireless WPA global key update interval
                                         (in 1000 packets)
[X] [X]     ssh                    --enable remote SSH access
[X] [X]     snmp                   --SNMP setting
[X] [X]       |-server             --enable SNMP agent
[X] [X]       |-trap server        --SNMP TrapServer IP address
[X] [X]       |-read community     --SNMP ReadCommunity
[X] [X]       |-write community    --SNMP WriteCommunity
[X] [X]       `-description        --SNMP System Description
[X] [X]     log                    --syslog setting
[X] [X]       |-client             --enable syslog client
[X] [X]       |-ipaddr             --syslog server IP address
[X] [X]       `-port               --syslog server port number
[X] [X]     http redirection       --HTTP Redirection setting
```

```
get set del keyword                  Description
--- --- --- ---------------------- -------------------------------
[X] [X]       |-server              --enable HTTP redirection
[X] [X]       `-url                --HTTP redirection URL
[X] [X] [X] wlan                   --wireless setting
[X] [X]       |-interface           --select wireless lan interface
[X]           |-version             --wireless driver version
[X] [X]       |-radio               --enable wireless radio
[X] [X]       |-wirelessmode        --wireless mode
[X] [X]       |-channel             --wireless channel (depends on country
              |                         and wireless mode)
[X] [X]       |-rate                --wireless transmission date rate
[X] [X]       |-power               --wireless transmit power
[X] [X]       |-fragmentationthreshold--wireless fragmentation threshold(even o
              |                       nly)
[X] [X]       |-rtsthreshold        --wireless RTS/CTS threshold
[X] [X]       |-super               --enable wireless super-A/G mode
[X] [X]       |-beaconinterval      --wireless beacon period in TU(1024 us)
[X] [X]       |-dtim                --wireless DTIM period in beacon interval
[X] [X]       |-preamble            --wireless preamble (only effect on
              |                         802.11b rates)
[X] [X]       |-operationmode       --wireless operation mode
[X] [X] [X]   |-remoteap            --wireless remote AP(s) (depends on
              |                         operationmode)
[X] [X] [X]   | |-p2p(+ap)          --remote AP address for p2p mode
[X] [X] [X]   | |-p2mp(+ap)         --remote AP address for p2mp mode
[X] [X] [X]   | | |-1               --1st remote AP address for p2mp mode
[X] [X] [X]   | | |-2               --2nd remote AP address for p2mp mode
[X] [X] [X]   | | |-3               --3rd remote AP address for p2mp mode
[X] [X] [X]   | | `-4               --4th remote AP address for p2mp mode
[X] [X] [X]   | `-repeater          --remote AP address for repeater mode
[X] [X] [X]   |   |-1               --1st remote AP address for repeater mode
[X] [X] [X]   |   |-2               --2nd remote AP address for repeater mode
[X] [X] [X]   |   |-3               --3rd remote AP address for repeater mode
[X] [X] [X]   |   `-4               --4th remote AP address for repeater mode
[X] [X] [X]   |-acl                 --wireless access control
[X] [X]       | |-mode              --enable wireless access control (ACL)
[X] [X] [X]   | `-list              --
        [X]   |   |-all             --(delete only) all local ACL address
[X] [X] [X]   |   `-(null)          --edit local ACL address
[X]           |-association         --list of associated wireless clients
[X]           |-wlanstats           --wlan statistics
[X] [X] [X]   |-key                 --wireless wep key setting
[X] [X]       | |-type              --wireless wep key type
[X] [X] [X]   | |-passphrase        --wireless wep passphrase key
[X] [X] [X]   | |-1                 --wireless wep key 1
[X] [X] [X]   | |-2                 --wireless wep key 2
[X] [X] [X]   | |-3                 --wireless wep key 3
```

```
get set del keyword                  Description
--- --- --- ---------------------- --------------------------------
[X] [X] [X]   | `-4                --wireless wep key 4
[X] [X]       |-wmm                --wmm settings
[X] [X] [X]   |-vap                --virtual ap infomation
[X] [X]       | |-index            --select vap index
[X] [X]       | |-active           --on/off this vap
[X] [X]       | |-profile name     --set vap profile name
[X]           | |-mac address      --vap mac address
[X] [X]       | |-ssid             --network name of this vap (1-32 chars)
[X] [X]       | |-ssidsuppress     --vap ssid broadcast suppress
[X] [X]       | |-wirelessisolate  --vap isolate communication between clients
[X] [X]       | |-authentication   --vap authentication type
[X] [X]       | |-encryption       --vap data encryption
[X] [X]       | |-default          --vap wep default key index
[X] [X] [X]   | |-psk              --vap pre-shared key (PSK) for WPA-PSK
[X] [X] [X]   | `-vlan entry       --set vlan entry infomation
[X] [X]       |   `-id             --
[X]           |-vlan list          --get vlan list
    [X]     password               --system password
    [X]     reboot                 --reboot system
    [X]     exit                   --logout from CLI
    [X]     quit                   --quit CLI
```

Index

Numerics

192.168.0.210, Static IP Address *2-4*

192.168.0.230, default address *2-4*

255.255.255.0
  default subnet *2-4*

3DES *3-2*

802.11a default name *2-9*

802.11a/g *1-4*

802.11b/g default name *2-9*

802.11e
  WMM *4-4*

802.1Q VLAN *1-2*, *2-7*
  enabling *2-13*

A

Access Controll screens *2-36*

Access Point name, default *2-12*

ACK *1-4*

Activity Log *3-3*

Activity Log screen *3-3*

Advailable Wireless Stations *2-37*

Advanced Access Point Settings screens *4-6*

Advanced IP Settings for Wireless Clients screen *4-1*

Advanced Wireless Settings screens *4-4*

AES *2-32*, *2-34*
  WPA2-PSK, use with *2-34*

Antenna
  2.4 GHz *1-8*
  5 GHZ *1-8*

antenna position *2-2*, *2-9*

Auto Uplink *1-3*, *1-5*

B

Backup/Restore Settings screen *3-12*

Basic Settings menu *2-7*

Basic Settings screen *2-11*

Beacon Interval
  default setting *4-5*

BSSID *1-2*

C

Carrier Sense Multiple Access with Collision Detection. See CSMA/CD.

Category 5 Ethernet cable *1-6*

Change Password screen *3-13*

channel
  interference,multiple access points
    channel spacing *2-2*

Channel/Frequency *2-14*, *2-16*

CLI *3-2*
  command set *3-3*
  command sets *C-1*

configuration
  erasing *3-13*
  restore *3-11*

configuration file
  backup and restore settings *3-11*
  retrieving *3-12*
  saving *3-12*

crossover cable *1-5*

CSMA/CD *4-5*

D

Data Encryption
  AES *2-32*, *2-34*

TKIP *2-31*
TKIP+AES *2-33*, *2-35*
Data Rate *2-15*, *2-16*
Daylight Saving Time
adjustment for *2-13*
default login *2-4*
default password *2-4*, *2-11*
Default Settings *A-1*
default settings *2-17*
default subnet mask
255.255.255.0 *2-4*
default user name *2-4*, *2-11*
DHCP Client *1-2*, *2-13*
enabling *2-13*
DHCP Server
enabling access point *4-1*
use as *4-1*
DHCP wireless clients
settings of *4-1*
DTIM Interval
default setting *4-5*
dynamic IP addresses
enabling *2-9*

E

emulation program settings
Telnet, use with *3-2*
Enable SysLog *3-4*
equipment placement
reception range *2-1*
Ethernet
Autosensing connection *1-3*
LAN *1-8*
Layer 3 managed switcfh *1-3*
Power over *1-3*
RJ-45 port *1-8*

F

factory default settings
reset button *1-8*, *5-4*
resetting *5-4*
restoring *3-13*
features *1-2*
firmware, upgrading *1-3*
Fragmentation Length
default setting *4-5*
front panel
diagram of *1-6*

G

Gateway
default address *2-13*
general information screen
field descriptions *3-5*
General Summary screen *3-5*

H

hotspot
setting up server *4-3*
settings *1-3*
Hotspot settings *4-1*
Hotspot Settings screen *4-3*
hotspots *2-31*, *2-33*, *2-34*, *2-35*, *2-36*
WIreless Client Security Separation *2-29*
http
//192.168.0.230 *2-10*
HTTP redirect, enabling *4-1*

I

interference sources *2-2*
IP Address
default *2-10*
IP address
default *2-10*, *2-13*, *2-17*
IP Address, settings *2-7*
IP Settings
DHCP clients *4-1*
DHCP server, use of *4-1*
Static IP clients *4-1*
IP Subnet mask
default *2-13*

L

LAN IP address
default *2-36*, *5-3*
LED indicators
table of *1-7*
Login screen *2-4*
login screen *2-11*

M

MAC address *2-36*
restricting access *2-3*
trusted PCs *2-3*
MAC Address Database
Local *2-36*
RADIUS *2-36*
Mode
SuperA, enabling *4-4*
SuperG, enabling *4-4*
mode
SuperA *4-4*
SuperG *4-4*
multiple access points
placement of *2-2*

N

NetBIOS *2-12*
Network Authentication *2-20*
types of *2-20*
Network Key. See passphrase.
null-modem cable *3-2*

O

Output Power *2-15*, *2-17*

P

package contents *1-5*
Packet fragmentation *1-4*
passphrase
use with WEP *2-29*
WPA2-PSK, use with *2-34*
WPA-PSK/WPA2-PSK, use with *2-35*
password
default *2-11*, *2-17*, *2-36*
performance degradation
causes of *2-2*
point-to-multi-point bridge *4-5*
configuring *4-8*
point-to-multi-point bridge. *1-3*
point-to-point bridge *1-3*, *4-5*
configuring *4-7*
power adapter *1-8*
Preamble Type
defalt setting *4-5*
Primary DNS Servers
default *2-13*
Private Community Name
default name *3-2*
Public Community Name
default setting *3-2*

Q

QoS. See Quality of Service *1-4*
Quality of Service *1-4*

R

RADIUS Server *2-18*
Range *2-1*
rear panel
diagram of *1-8*
Reboot *3-13*, *5-4*
Receive Traps *3-2*
reception range
equipment placement *2-1*
Remote Console *3-1*
Remote Console Secure Shell *3-2*
remote management
via Telenet *3-1*
Remote Management screen *3-1*
Repeater *4-6*

repeater mode
enabling *4-1*
Repeater, wireless
configuring *4-9*
Reset to Factory Defaults *3-13*
restore configuration *3-11*
restore default settings *3-13*
restricting access
MAC address, using *2-36*
RTS Threshold
default setting *4-5*
RTS/CTS handshake *1-4*

S

Secondary DNS Servers
default *2-13*
security
network enhancements *2-3*
WPA *2-3*
WPA-PSK *2-3*
security options
WEP data encryption *2-3*
WPA-PSK *2-3*
Security Profile
use with WPA/WPA2 with RADIUS *2-33*
use with WPA2 with RADIUS *2-31*
with WPA *2-30*
security profile
about *2-18*
default settings *2-17*
Security Profile Name *2-19*
Security Profiles
screens *2-18*
serial
DTE connection *1-8*
port *1-8*
serial console
port *1-8*
SNMP *1-2*, *3-1*
default setting *3-2*
software upgrade *3-10*
Spanning Tree Protocol
enabling *2-13*
SSH. See Remote Console Secure Shell.
SSH1 *3-2*
SSID *1-3*, *2-18*, *3-5*, *3-6*
11a default name *2-19*
11b/g default name *2-19*
802.11a default *2-9*
802.11b/g default *2-9*
disabling, consequences of *2-3*
Static IP Address, 192.168.0.210 *2-4*
Static IP Wireless clients
settings for *4-1*
Statistics
field descriptions *3-8*
screen *3-8*
Subnet Mask
default *5-3*
supported standards *1-2*
SysLog Port *3-4*
SysLog server *3-3*
SysLog Server IP address *3-4*
system requirements *1-5*

T

TCP/IP
configuration for DHCP server *4-2*
Technical Specifications *A-3*
Telnet
3DES *3-2*
CLI *1-3*
SSH1 *3-2*
using CLI *3-2*
Telnet client
recommendations *3-2*
Telnet console *3-1*
Time Zone *2-13*
TKIP *2-31*, *2-34*
TKIP+AES *2-33*, *2-35*
troubleshooting *5-1*
access point, connecting to *5-3*
configuring, *5-3*

LAN activity *5-2*
power connection *5-1*
timeout error *5-3*
wireless Internet connection *5-2*
wireless LAN activity l *5-2*

Trusted Wireless Stations *2-36*, *2-37*

trusted wireless stations
MAC address filtering, use with *1-3*

Turn Access Control On *2-36*

Turn Radio On *2-14*, *2-16*

U

Upgrade Firmware screen *3-11*

user name
default *2-11*, *2-17*, *2-36*

V

VLAN
IDs *1-4*
security profiles *1-4*

VT100/ANSI
terminal, connecting *3-2*
workstation, connecting *3-2*

W

WEP *2-3*

Wi-Fi MultimediaWMM. See Wi-Fi Multimedia.

Wireless
point-to-multi-point bridge *4-5*
point-to-point bridge *4-5*

wireless access point
default name *2-9*
deployment of *2-9*
verifying connectivity *2-9*

wireless bridge, enabling *4-1*

Wireless Client Security Separation *2-29*, *2-32*, *2-33*, *2-34*, *2-35*, *2-36*

wireless configuring
80211.a mode *2-14*
80211.b/g modes *2-14*

wireless connectivity
testing *2-17*
testing Wireless Settings 11a *2-17*
testing Wireless Settings 11b/g *2-17*

Wireless Mode *2-14*, *2-16*

Wireless Multimedia *1-4*

Wireless Network Name. See SSID

Wireless Repeater *1-3*

wireless security
options *2-2*

wireless settings
11a *2-8*
11b/g *2-8*
configuring 802.11a *2-14*
configuring 802.11b/g *2-15*
screen *2-14*

Wireless Settings 11a screen *2-14*

Wireless Settings 11b/g screen *2-15*

wireless settings screen
11a *2-8*
11b/g *2-8*

Wireless Station
adding new *2-37*

Wireless Station List screen *3-10*

WPA *2-3*
use restrictions *2-20*

WPA and WPA2 with RADIUS
configuration of *2-32*
Network Authentication screens *2-32*
restrictions *2-32*
TKIP+AES *2-33*

WPA with RADIUS
configuration of *2-30*
Network Authentication screen *2-30*
restrictions *2-30*
security profiles *2-30*
TKIP *2-31*

WPA2
use restrictions *2-20*

WPA2 with RADIUS
AES *2-32*
configuration of *2-31*
Network Authentication screen *2-31*
restructions *2-31*

security profiles *2-31*

WPA2-PSK
- AES *2-34*
- configuration of *2-34*
- Network Authentication screens *2-34*
- restrictions *2-34*

WPA-PSK *2-3*
- configuration of *2-33*
- Network Authentication screens *2-33*
- restrictions *2-33*
- TKIP *2-34*

WPA-PSK and WPA2-PSK
- configuration of *2-35*
- Network Authentication screens *2-35*
- restructions *2-35*

WWM. See Wireless Multimedia.